IWE1200A-G

USER'S MANUAL

IEEE 802.11b
Hotspot Access Gateway
(Wired and Wireless Editions)

User's Guide

Version: 1.8

Last Updated: 11/24/2004

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiated radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Portugal, Spain, Sweden, The Netherlands, and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Norway and Switzerland.

EU Countries Not Intended for Use

None.

Table of Contents

1. Introduction

1.1. Overview

The IEEE 802.11b Hotspot Access Gateway enables wireless ISPs, enterprises, or schools to deploy WLANs with user authentication support. Authentication can be achieved using the *Web redirection* technology or IEEE 802.1x Port-Based Network Access Control.

Based on the Web redirection technology, when an unauthenticated wireless user is trying to access a Web page, a logon page is shown instead of the requested page, so that the user can type his/her user name and password for authentication. Based on IEEE 802.1x, after a wireless client computer associates with the built-in access point of the access gateway, the wireless client computer uses the logged-on user's *user credential* for authentication. The user credential can be user name/password (if EAP-MD5 is used) or digital certificate (if EAP-TLS is used).

After the access gateway acquires the user credential either through Web redirection or IEEE 802.1x, it sends the user credential to a back-end RADIUS (Remote Authentication User Dial-In Service) server to see if the wireless user is allowed to access the Internet. Furthermore, if a user is IEEE 802.1x EAP-TLS authenticated, wireless data transmitted between the access gateway and the wireless client computer can be encrypted for better security.

In Chapter 2, we describe the steps to install and configure a newly acquired WLAN hotspot access gateway. Following the steps, the WLAN hotspot access gateway can be quickly set up to work. In Chapter 3, detailed explanations of each Web management page are given for the user to understand how to fine-tune the settings of a WLAN hotspot access gateway to meet his or her specific needs. In the remainder of this guide, a WLAN hotspot access gateway is referred to as a *gateway* for short.

1.2. Features

- **User Authentication, Authorization, and Accounting (AAA)**
  - **Web redirection.** When an unauthenticated wireless user is trying to access a Web page, he/she is redirected to a logon page for entering the user name and password. Then, the user credential information is sent to a back-end RADIUS server for authentication.
    - **Local pages or external pages.** The access gateway can be configured to use *log-on*, *log-off*, *authentication success*, and *authentication failure* pages, which are stored in itself or stored in an external Web server maintained by the WISP. The contents of local authentication pages can be customized.
    - **CGI-Based Authentication.** Username/password information can be sent by directly calling a CGI (Common Gateway Interface) function on the access gateway. This feature is useful for authentication automation achieved by a specifically designed program running on the wireless client computer.
    - **Advertisement links.** The *log-off* authentication page can be configured to show a sequence of advertisement banners.
    - **Unrestricted clients.** Client computers with specific IP addresses or MAC addresses can bypass the Web redirection-based access control. The MAC address list can be uploaded by TFTP.

        - **Walled garden.** Some specific URLs can be accessed without authentication. These URLs can be exploited by WISPs for advertisement purposes.

        - **SSL username/password protection.** Username/password information sent by a wireless client to the access gateway can be encrypted by SSL (Secure Socket Layer).

    - **IEEE 802.1x.** If a wireless client computer supports IEEE 802.1x Port-Based Network Access Control, the user of the computer can be authenticated by the access gateway and wireless data can be encrypted when the digital-certificate-based EAP-TLS authentication method is selected.

    - **RADIUS client.** The WLAN hotspot access gateway communicates with a back-end RADIUS server for wireless user authentication, authorization, and accounting. Authentication methods, including EAP-MD5, EAP-TLS/EAP-TTLS, PAP, and CHAP are supported.

        - **Robustness.** To enhance AAA integrity, the access gateway can be configured to notify the RADIUS server after it reboots.

        - **Showing authenticated users.** Showing the status and statistics of every RADIUS-authenticated user. And an authenticated user can be terminated at any time for management purposes.

    - **Authentication session control.** Several mechanisms are provided for the network administrator to control user authentication session lifetimes.

- **IEEE 802.11b**

    - **Access point.** The wireless access gateway is equipped with a built-in Access Point (AP), which bridges packets between the wireless IEEE 802.11b network interface and the wired Ethernet interface

    - **64-bit and 128-bit WEP (Wired Equivalent Privacy).** For authentication and data encryption.

    - **Enabling/disabling SSID broadcasts.** The user can enable or disable the SSID broadcasts functionality for security reasons. When the SSID broadcasts functionality is disabled, a client computer cannot associate the wireless AP with an “any” network name (SSID, Service Set ID); the correct SSID has to be specified on client computers.

    - **MAC-address-based access control.** Blocking unauthorized wireless client computers based on MAC (Media Access Control) addresses.

    - **Repeater.** A wireless AP can communicate with other wireless APs via WDS (Wireless Distribution System). Therefore, the wireless AP can wirelessly forward packets from wireless clients to another wireless AP, and then the later wireless AP forwards the packets to the Ethernet network.

    - **Wireless client isolation.** Wireless-to-wireless traffic can be blocked so that the wireless clients cannot see each other. This capability can be used in hotspots applications to prevent wireless hackers from attacking other wireless users’ computers.

    - **AP load balancing.** Several wireless APs can form a load-balancing group. Within a group, wireless client associations and traffic load can be shared among the wireless APs.

- **Transmit power control.** Transmit power of the wireless AP's RF module can be adjusted to change RF coverage of the wireless AP.

- **Associated wireless clients status.** Showing the status of every wireless client that is associated with the wireless AP.

- **Detachable antennas.** The factory-mounted antennas can be replaced with high-gain antennas for different purposes.

- **Internet Connection Sharing**

  - **DNS proxy.** The WLAN hotspot access gateway can forward DNS (Domain Name System) requests from client computers to DNS servers on the Internet. And DNS responses from the DNS servers can be forwarded back to the client computers.

    - **Host address resolution.** The network administrator can specify static FQDN (Fully Qualified Domain Name) to IP address mappings. Therefore, a host on the internal network can access a server also on the intranet by a registered FQDN.

  - **DHCP server.** The WLAN hotspot access gateway can automatically assign IP addresses to client computers by DHCP (Dynamic Host Configuration Protocol).

    - **Static DHCP mappings.** The network administrator can specify static IP address to MAC address mappings so that the specified IP addresses are always assigned to the hosts with the specified MAC addresses.

    - **Showing current DHCP mappings.** Showing which IP address is assigned to which host identified by an MAC address.

  - **NAT server.** Client computers can share a public IP address provided by an ISP (Internet Service Provider) by NAT (Network Address Translation). And our NAT server functionality supports the following:

    - **Virtual server.** Exposing servers on the intranet to the Internet.

    - **PPTP, IPSec, and L2TP passthrough.** Passing VPN (Virtual Private Network) packets through the intranet-Internet boundary. PPTP means Point-to-Point Tunneling Protocol, IPSec means IP Security, and L2TP means Layer 2 Tunneling Protocol.

    - **DMZ (DeMilitarized Zone).** All unrecognized IP packets from the Internet can be forwarded to a specific computer on the intranet.

    - **Multiple public IP addresses support.** An ISP may provide several public IP addresses to a customer. The WLAN hotspot access gateway can map each of the public IP addresses to a host with a private IP address on the intranet.

    - **H.323 passthrough.** Passing H.323 packets through the intranet-Internet boundary so that users on the intranet can use VoIP (Voice over IP) applications.

    - **MSN Messenger support.** Supporting Microsoft MSN Messenger for chat, file transfer, and real-time communication applications.

    - **Session monitoring.** Latest 50 incoming sessions and 50 outgoing sessions are shown for monitoring user traffic.

- **DSL/Cable Modem Support.** Supporting dynamic IP address assignment by PPPoE

(Point-to-Point Protocol over Ethernet) or DHCP and static IP address assignment.

  - **Multiple DSL/Cable connections support.** Supporting up to 4 DSL/cable-based Internet connections. All outgoing traffic load from the internal network is shared among the multiple Internet connections, so that total outgoing throughput is increased.

    - **Load balancing control.** Specific LAN-to-WAN traffic can be forced to go out to the Internet through a specific Internet connection. LAN-to-WAN traffic can be classified *by port range* or *by IP address range*.

    - **Bandwidth control.** Network bandwidth consumed by each client can be limited. Clients are identified by *MAC address range* or *IP address range*.

  - **Zero client reconfiguration.** The access gateway can be configured to ignore IP, DNS, and/or SMTP (Simple Mail Transfer Protocol) settings of client computers. As a result, the configuration of a client computer need not be changed to access the Internet through the access gateway.

- **Network Security**

  - **Packet address and port filtering.** Filtering outgoing packets based on IP address and port number. (Incoming packet filtering is performed by NAT.)

  - **URL filtering.** Preventing client users from accessing unwelcome Web sites. The HTTP (HeperText Transfer Protocol) traffic to the specified Web sites identified by URLs (Universal Resource Locators) is blocked.

  - **WAN ICMP requests blocking.** Some DoS (Denial of Service) attacks are based on ICMP requests with large payloads. Such kind of attacks can be blocked.

  - **Stateful Packet Inspection (SPI).** Analyzing incoming and outgoing packets based on a set of criteria for abnormal content. Therefore, SPI can detect hacker attacks, and can summarily reject an attack if the packet fits a suspicious profile.

  - **Wireless-to-Ethernet-LAN traffic blocking.** Traffic between the wireless interface and the Ethernet LAN interface can be blocked.

- **Changeable MAC Address of the Ethernet WAN Interface.** Some ADSL modems work only with Ethernet cards provided by the ISP. If a WLAN hotspot access gateway is used in such an environment, the MAC address of the WAN interface of the gateway has to be changed to the MAC address of the ISP-provided Ethernet network card.

- **SNTP.** Support for absolute system time by SNTP (Simple Network Time Protocol).

  - **Daylight saving time.** Support for *Daylight Saving Time*.

- **Dynamic DNS.** Support for dynamic DNS services provided by *dyndns.org* and *no-ip.com*, so that the access gateway can be associated with a domain name even if it obtains an IP address dynamically by PPP, PPPoE or DHCP.

- **LAN Device Management.** Since the access gateway acts as an NAT server, to remotely manage network devices (such as access points) on the private network needs special handling, so that management packets from the Internet can be passed through the NAT server. The access gateway supports two mechanisms for this purpose.

- **By NAT port mapping.** By carefully configuring the NAT port mapping table, the access gateway knows how to route management packets with specific IP ports to LAN devices on the private network. Although the NAT Virtual Server function can be used for this purpose, the access gateway is equipped with specific configuration pages for LAN device management.

- **By PPTP and virtual second LAN.** Alternatively, LAN device management can be achieved by PPTP and *virtual second LAN*. Conceptually, wireless clients are in the *physical first LAN* within one IP subnet (ex. 192.168.0.xxx) and wireless access points that extend RF coverage are in the *virtual second LAN* within another IP subnet (ex. 10.0.0.xxx). These two LANs are isolated by the access gateway so that no traffic between these two LANs is allowed. After the built-in PPTP client of the access gateway establishes a PPTP tunnel with a remote PPTP server, the access gateway can route packets between the PPTP tunnel and the virtual second LAN. This way, the network administrator can manage the access points on the virtual second LAN through the PPTP tunnel.

- **Firmware Tools**

  - **Firmware upgrade.** The firmware of the WLAN hotspot access gateway can be upgraded in the following methods:

    - **Xmodem-based.** Upgrading firmware over RS232.

    - **TFTP-based.** Upgrading firmware by TFTP (Trivial File Transfer Protocol).

    - **HTTP-based.** Upgrading firmware by HTTP (HeperText Transfer Protocol).

  - **Configuration backup.** The configuration settings of the WLAN hotspot access gateway can be backed up to a file via TFTP or HTTP for later restoring.

  - **Configuration reset.** Resetting the configuration settings to factory-default values.

- **Management**

  - **Web-based Network Manager** for configuring and monitoring the WLAN hotspot access gateway via a Web browser. The management protocol is HTTP (HeperText Transfer Protocol)-based. The access gateway can be configured to be managed:

    - Only from the LAN side.
    - Both from the LAN side and WAN side.
    - Only from the WAN side.

    In addition, it can also be configured to accept management commands only from specific hosts.

  - **UPnP.** The access gateway responds to UPnP discovery messages so that a Windows XP user can locate the access gateway in My Network Places and use a Web browser to configure it.

  - **SNMP.** SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, IEEE 802.1x, Private Enterprise MIB are supported.

  - **System log.** For system operational status monitoring.

    - **Local log.** System events are logged to the on-board RAM of the access gateway and can be viewed using a Web browser.

        - **Remote log by SNMP trap.** Systems events are sent in the form of SNMP traps to a remote SNMP management server.

- **Auto Recovery.** In rare cases, the firmware of the access gateway gets stuck in an invalid state and the access gateway appears to be locked up from end user perspective. The access gateway provides the following mechanisms to automatically recover from the lockup situation, so that availability is enhanced:

    - **Link integrity detection.** The access gateway periodically checks the connectivity between a reference host and itself. If the connectivity is broken anyhow, the access gateway restarts automatically. This mechanism is aimed at solving lockup caused by firmware bugs in the TCP/IP stack of the access gateway.

    - **Periodical restart every day.** The access gateway can be configured to restart at a specific time every day. This mechanism is aimed at solving lockup caused by firmware bugs that surface only after the access gateway has operated for a long time.

    - **Hardware watchdog timer.** The access gateway firmware has to periodically reset the *hardware watchdog timer*. If it fails to do this, the hardware watchdog timer restarts the access gateway automatically. This mechanism is aimed at solving lockup caused by firmware bugs in the OS (operating system) of the access gateway.

- **LAN/WAN Configurable Ethernet Switch Ports.** The WLAN hotspot access gateway provides a 4-port Ethernet switch so that a stand-alone Ethernet hub/switch is not necessary for connecting Ethernet client computers to the gateway. These Ethernet ports can be configured as WAN ports for multiple DSL/cable-based Internet connections support.

1.3. Feature Comparison

	Wired Advanced	*Wireless Advanced*
IEEE 802.11 AP functionality		■
IEEE 802.1x		■
SNMP IEEE 802.1x MIB		■
Wireless client isolation		■
AP load balancing		■

1.4. LED Definitions

There are several LED indicators on the housing of the WLAN hotspot access gateway. They are defined as follows:

- **PWR**: *Power*
- **PPP**: *PPP/PPPoE*. Lights up when a PPP or PPPoE link has been established.
- **ALV**: *Alive*. Blinks when the gateway is working normally.
- **ST1-ST2**: Status 1 to 2 for status indication
- **WAN**: Ethernet WAN interface
    - **LNK**: *Link*. Lights up when the Ethernet WAN interface is initialized successfully.
    - **ACT**: *Active*. Lights up when the Ethernet WAN interface is transmitting or receiving data.
- **100/10 1-4**: 10/100 Ethernet LAN switch ports
    - **LNK**: *Link*. Lights up when an Ethernet cable is connected firmly to this Ethernet port.
    - **ACT**: *Active*. Lights up when this Ethernet port is transmitting or receiving data.

2. First-Time Installation and Configuration

2.1. Powering the WLAN Hotspot Access Gateway

1. Plug the power adapter to an AC socket.
2. Plug the connector of the power adapter to the power jack of the WLAN hotspot access gateway.

NOTE: This product is intended to be power-supplied by a Listed Power Unit, marked “Class 2” or “LPS” and output rated “5V DC, 1 A minimum” or equivalent statement.

2.2. Mounting the WLAN Hotspot Access Gateway on a Wall

The WLAN hotspot access gateway is wall-mountable.

1. Stick the supplied sticker for wall-mounting.
2. Use a ϕ7.0mm driller to drill a 25mm-deep hole at each of the cross marks.
3. Plug in a supplied plastic conical anchor in each hole.
4. Screw a supplied screw in each plastic conical anchor for a proper depth so that the WLAN hotspot access gateway can be hung on the screws.
5. Hang the WLAN hotspot access gateway on the screws.

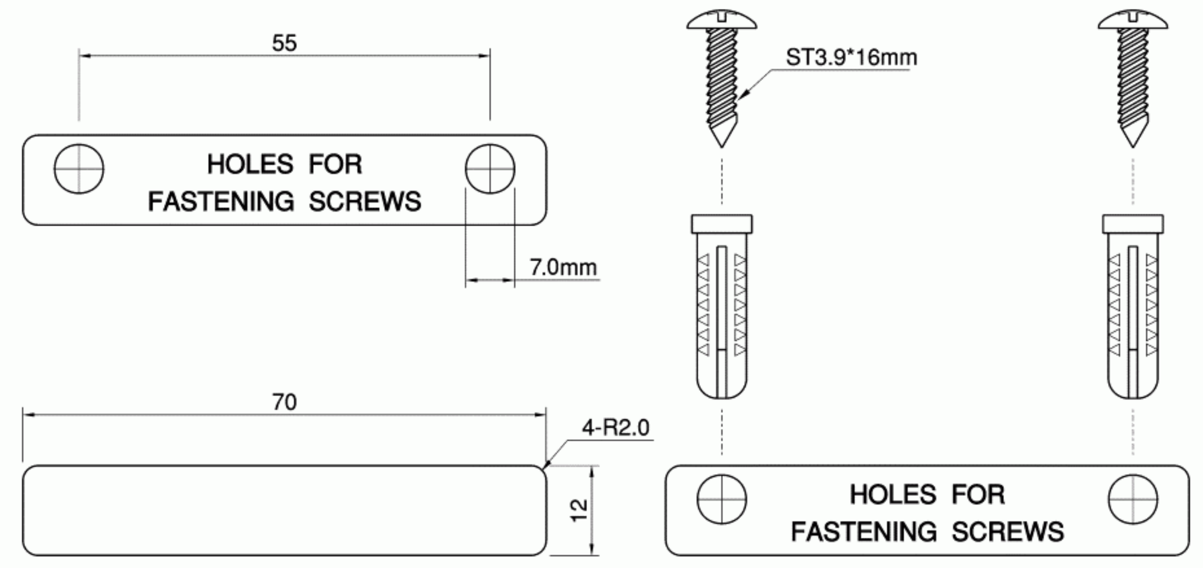


Fig. 1. Mounting the WLAN hotspot access gateway on a wall.

2.3. Preparing for Configuration

For you to configure a gateway, a *managing computer* with a Web browser is needed. For configuration of a gateway, an Ethernet network interface card (NIC) should have been installed in the managing computer.

NOTE: If you are using the browser, *Opera*, to configure a gateway, click the menu item **File**, click **Preferences...**, click **File types**, and edit the MIME type, **text/html**, to add a file extension ".sht" so that Opera can work properly with the Web management pages of the gateway.

Since the configuration/management protocol is HTTP-based, you have to make sure that **the IP address of the managing computer and the IP address of the *managed gateway* are in the same IP subnet**. By default (see Appendix A-1, "Default Settings"), the DHCP server functionality of a gateway is enabled, so that if the managing computer is set to automatically obtain an IP address by DHCP, the condition can be satisfied easily.

2.3.1. Connecting the Managing Computer and the WLAN Hotspot Access Gateway

Connect the Ethernet managing computer to anyone of the LAN switch ports of the managed gateway with a *normal* Ethernet cable (see Fig. 2).

NOTE: There are two types of Ethernet cables—*normal* and *crossover*.

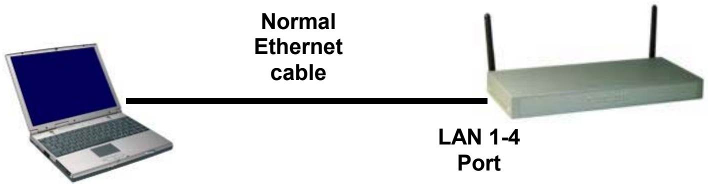


Fig. 2. Connecting a managing computer and a WLAN hotspot access gateway via Ethernet.

Since the DHCP server functionality is factory-set to be enabled, it's recommended that there are no other computers connected to the other Ethernet switch ports of the gateway, so that you can be 100-percent sure that the gateway will be the DHCP server of the managing computer.

2.3.2. Changing the TCP/IP Settings of the Managing Computer

Use the **Windows Network Control Panel Applet** to change the TCP/IP settings of the managing computer, so that the IP address of the computer and the IP address of the gateway are in the same IP subnet. If the managing computer is originally set a static IP address, you can either change the IP address to **192.168.0.xxx** (the default IP address of a gateway is **192.168.0.1**) and the subnet mask to **255.255.255.0** or select an automatically-obtain-an-IP-address option.

TIP: You can use Wireless Router/AP Browser on the companion CD-ROM to scan for all the gateways on the network. Double-click a scanned gateway to launch the default Web browser to manage the gateway.

NOTE: On Windows 2000/XP, Wireless Router/AP Browser can only be run by a user with administrator privilege.

NOTE: For some versions of Windows, the computer needs to be restarted for the changes of TCP/IP settings to take effect.

If the computer is already set to obtain an IP address automatically, you can use the Windows-provided tool, **WinIPCfg.exe** (on Windows 9x/Me) or **IPConfig.exe** (on Windows 2000/XP), to re-obtain an IP address from the gateway. **WinIPCfg.exe** is a GUI program, and has command buttons for releasing the current IP address and re-obtaining an IP address. **IPConfig.exe** is a command-line program, and the **/release** option releases the current IP address and the **/renew** option triggers the Windows DHCP client subsystem to re-obtain an IP address.

NOTE: By default, the first assignable IP address of the DHCP server on the gateway is **192.168.0.2**.

2.4. Configuring the WLAN Hotspot Access Gateway

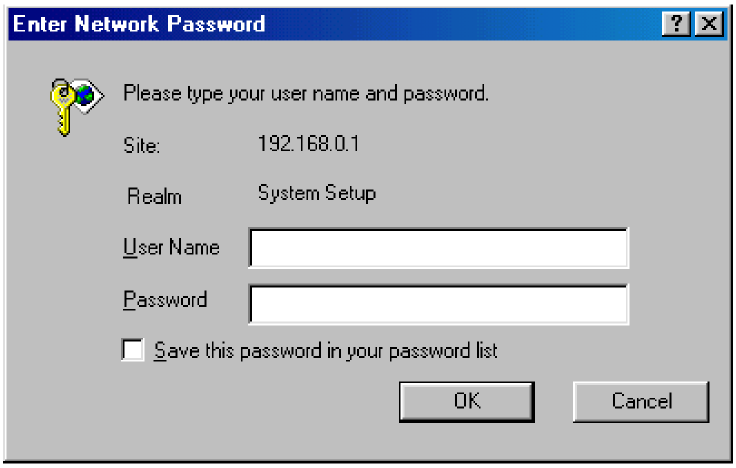
After the IP addressing issue is resolved, launch a Web browser on the managing computer. Then, go to "**http://192.168.0.1**" to access the *Web-based Network Manager* start page.

NOTE: If you are using the browser, *Opera* (from Opera Software), to configure a gateway, click the menu item **File**, click **Preferences...**, click **File types**, and edit the MIME type, **text/html**, to add a file extension ".sht" so that Opera can work properly with the Web management pages of the gateway.

TIP: For maintenance configuration of a gateway, the gateway can be reached by its *host name* using a Web browser. For example, if the gateway is named "gateway", you can use the URL "http://gateway" to access the Web-based Network Manager of the gateway.

2.4.1. Entering the User Name and Password

Before the start page is shown, you will be prompted to enter the user name and password to gain the right to access the Web-based Network Manager. For first-time configuration, use the default user name "**root**" and default password "**root**", respectively.



Enter Network Password

Please type your user name and password.

Site: 192.168.0.1

Realm System Setup

User Name

Password

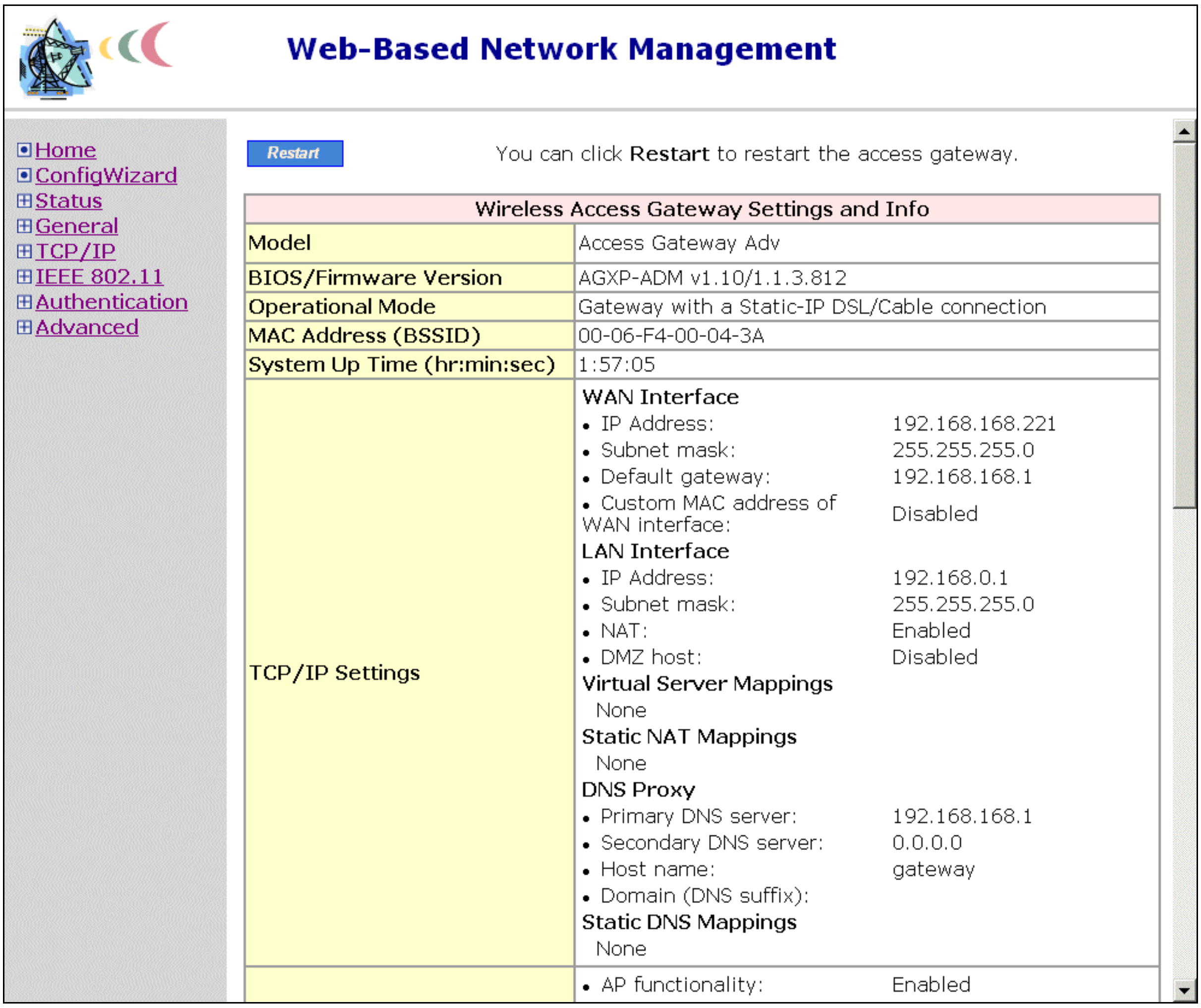
□ Save this password in your password list

Fig. 3. Entering the user name and password.

NOTE: It is strongly recommended that the password be changed to other value for security reasons. On the start page, click the **General, Password** link to change the value of the password (see Section 3.3.2 for more information).

TIP: Since the start page shows the current settings and status of the gateway, it can be saved or printed within the Web browser for future reference.

On the start page, click the **ConfigWizard** link to use a configuration wizard to quickly change the configuration of the gateway.



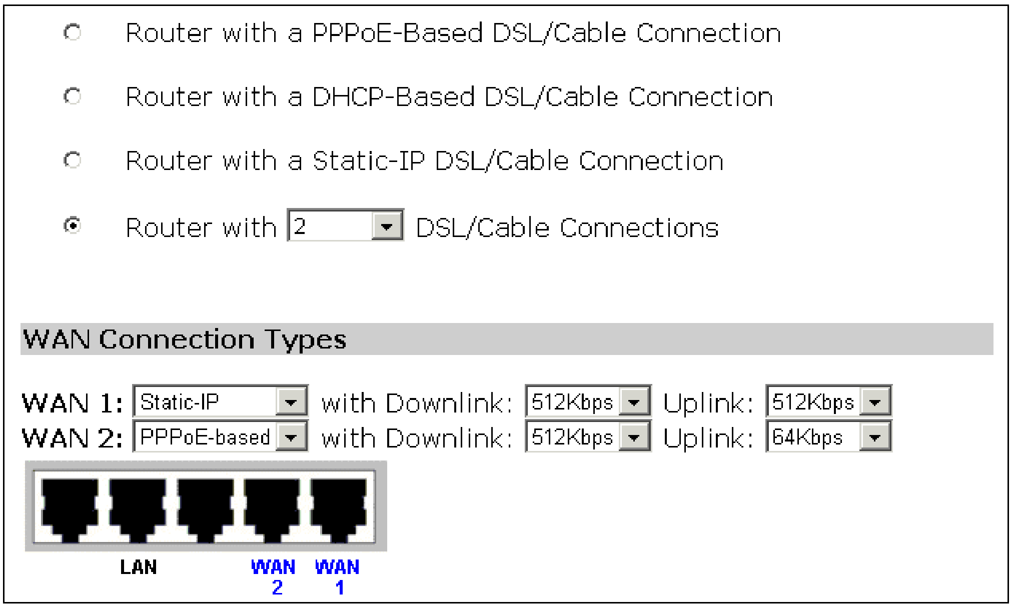
You can click **Restart** to restart the access gateway.

Wireless Access Gateway Settings and Info	
Model	Access Gateway Adv
BIOS/Firmware Version	AGXP-ADM v1.10/1.1.3.812
Operational Mode	Gateway with a Static-IP DSL/Cable connection
MAC Address (BSSID)	00-06-F4-00-04-3A
System Up Time (hr:min:sec)	1:57:05
TCP/IP Settings	WAN Interface • IP Address: 192.168.168.221 • Subnet mask: 255.255.255.0 • Default gateway: 192.168.168.1 • Custom MAC address of WAN interface: Disabled LAN Interface • IP Address: 192.168.0.1 • Subnet mask: 255.255.255.0 • NAT: Enabled • DMZ host: Disabled Virtual Server Mappings None Static NAT Mappings None DNS Proxy • Primary DNS server: 192.168.168.1 • Secondary DNS server: 0.0.0.0 • Host name: gateway • Domain (DNS suffix): Static DNS Mappings None
	• AP functionality: Enabled

Fig. 4. The Start page.

The first page of the configuration wizard is a welcome page. This page gives a brief description of the configuration process. Click **Next** to continue. We'll explain what to do step-by-step in the following subsections.

2.4.2. ConfigWizard Step 1: Selecting an Operational Mode



○ Router with a PPPoE-Based DSL/Cable Connection

○ Router with a DHCP-Based DSL/Cable Connection

○ Router with a Static-IP DSL/Cable Connection

● Router with 2 DSL/Cable Connections

WAN Connection Types

WAN 1: Static-IP with Downlink: 512Kbps Uplink: 512Kbps

WAN 2: PPPoE-based with Downlink: 512Kbps Uplink: 64Kbps

Fig. 5. Operational modes.

- If the gateway is to be used with a DSL or cable modem and the IP address assignment for the Ethernet WAN interface is achieved by PPPoE, select **Gateway with a PPPoE-Based DSL/Cable Connection**.

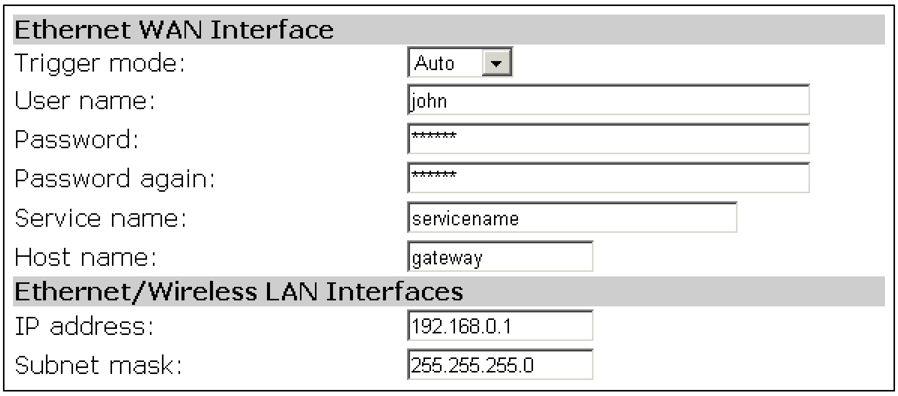
- If the gateway is to be used with a DSL or cable modem and the IP address assignment for the Ethernet WAN interface is achieved by DHCP, select **Gateway with a DHCP-Based DSL/Cable Connection**.

- If the gateway is to be used with a DSL or cable modem and the IP address of the Ethernet WAN interface has to be manually set, select **Gateway with a Static-IP DSL/Cable Connection**.

- If you have multiple ADSL/cable connections, select **Gateway with *n* DSL/Cable Connections**. Select the number of connections using the drop-down list, and then specify the type, downlink date rate and uplink data rate of each ADSL/cable connection. The specified data rates affect the load-balancing engine of the gateway.

2.4.3. ConfigWizard Step 2: Configuring TCP/IP Settings

2.4.3.1. Gateway with a PPPoE-Based DSL/Cable Connection



Ethernet WAN Interface

Trigger mode: Auto

User name: john

Password: ******

Password again: ******

Service name: servicename

Host name: gateway

Ethernet/Wireless LAN Interfaces

IP address: 192.168.0.1

Subnet mask: 255.255.255.0

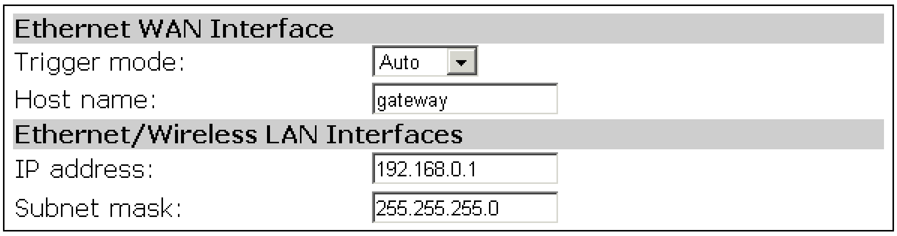
Fig. 6. TCP/IP settings for **Gateway with a PPPoE-Based DSL/Cable Connection** mode.

If the gateway was set to be in **Gateway with a PPPoE-Based DSL/Cable Connection** mode, two IP addresses are needed—one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained automatically by PPPoE from the ISP. Consult your ISP for the correct **User name**, **Password**, and **Service name** settings.

The **Trigger mode** setting specifies the way a PPPoE connection is established. Your PPPoE connection can be established and torn down *manually* (**Manual**) by clicking the **Connect** and **Disconnect** buttons on the Start page, respectively. Or you can choose to let the device *automatically* (**Auto**) establish a PPPoE connection at bootup time. In **Auto** mode, if the connection is disrupted, the device will try to re-establish the broken connection automatically.

2.4.3.2. Gateway with a DHCP-Based DSL/Cable Connection



Ethernet WAN Interface

Trigger mode: Auto

Host name: gateway

Ethernet/Wireless LAN Interfaces

IP address: 192.168.0.1

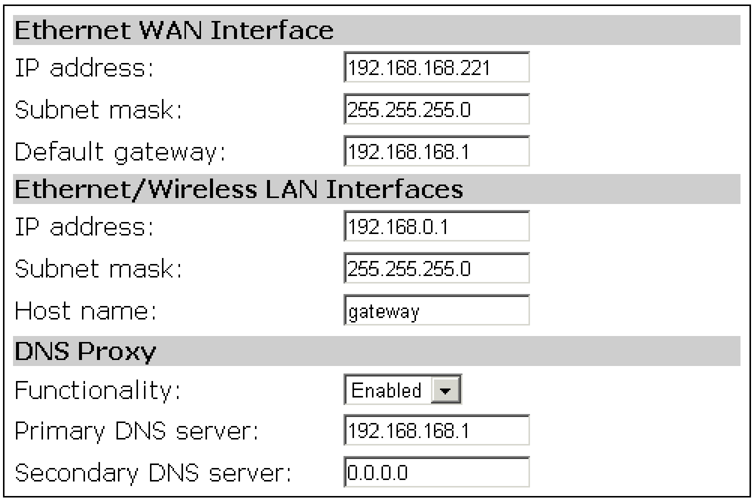
Subnet mask: 255.255.255.0

Fig. 7. TCP/IP settings for **Gateway with a DHCP-Based DSL/Cable Connection** mode.

If the gateway was set to be in **Gateway with a DHCP-Based DSL/Cable Connection** mode, two IP addresses are needed—one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained by DHCP from the ISP. The **Trigger mode** setting affects the behavior of the DHCP client of the gateway. In **Auto** mode, you don't have to worry about the DHCP process; the device takes care of everything. In **Manual** mode, there are two buttons on the Start page for you to manually release an obtained IP address (**Release**) and re-obtain a new one from a DHCP server (**Renew**).

2.4.3.3. Gateway with a Static-IP DSL/Cable Connection



Ethernet WAN Interface

IP address: 192.168.168.221

Subnet mask: 255.255.255.0

Default gateway: 192.168.168.1

Ethernet/Wireless LAN Interfaces

IP address: 192.168.0.1

Subnet mask: 255.255.255.0

Host name: gateway

DNS Proxy

Functionality: Enabled

Primary DNS server: 192.168.168.1

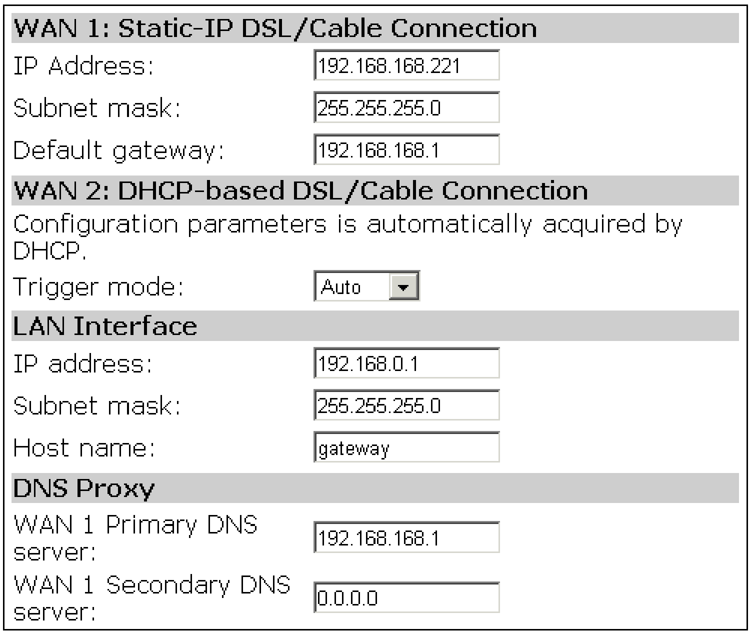
Secondary DNS server: 0.0.0.0

Fig. 8. TCP/IP settings for **Gateway with a Static-IP DSL/Cable Connection** mode.

If the gateway was set to be in **Gateway with a Static-IP DSL/Cable Connection** mode, two IP addresses are needed—one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it must be manually set. Consult your ISP for the correct **IP address**, **Default gateway**, **Subnet mask**, **Primary DNS server**, and **Secondary DNS server** settings.

2.4.3.4. Gateway with Multiple DSL/Cable Connections



WAN 1: Static-IP DSL/Cable Connection

IP Address:	192.168.168.221
Subnet mask:	255.255.255.0
Default gateway:	192.168.168.1

WAN 2: DHCP-based DSL/Cable Connection

Configuration parameters is automatically acquired by DHCP.

Trigger mode:	Auto

LAN Interface

IP address:	192.168.0.1
Subnet mask:	255.255.255.0
Host name:	gateway

DNS Proxy

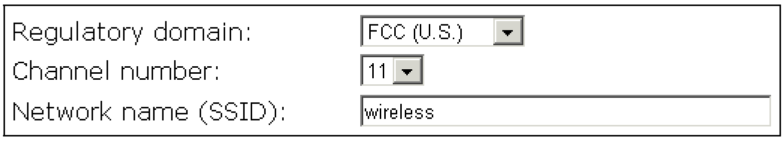
WAN 1 Primary DNS server:	192.168.168.1
WAN 1 Secondary DNS server:	0.0.0.0

Fig. 9. TCP/IP settings for **Gateway with Multiple DSL/Cable Connections** mode.

Since the Internet connection can be PPPoE-based, DHCP-based, or Static-IP-based, the addressing settings of each WAN interface are the same as those of **Gateway with a PPPoE-Based DSL/Cable Connection**, **DHCP-Based DSL/Cable Connection**, or **Gateway with a Static-IP DSL/Cable Connection**, respectively. As a result, refer to Sections 2.4.3.1, 2.4.3.2, and 2.4.3.3 for more information.

2.4.4. ConfigWizard Step 3: Configuring IEEE 802.11 Settings

IEEE 802.11b-related communication settings include **Regulatory domain**, **Channel number**, and **Network name (SSID)**.

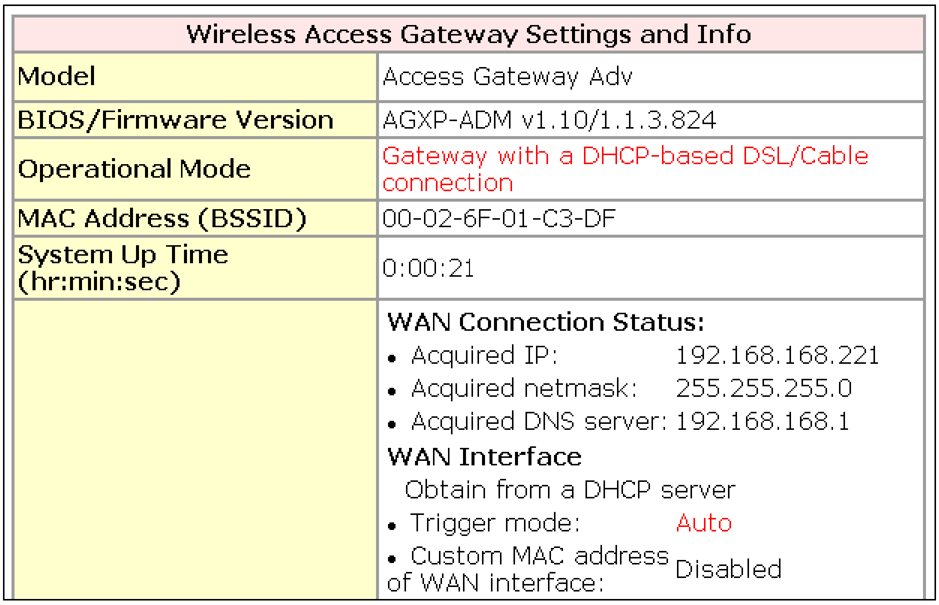


Regulatory domain:	FCC (U.S.)
Channel number:	11
Network name (SSID):	wireless

Fig. 10. IEEE 802.11b communication settings.

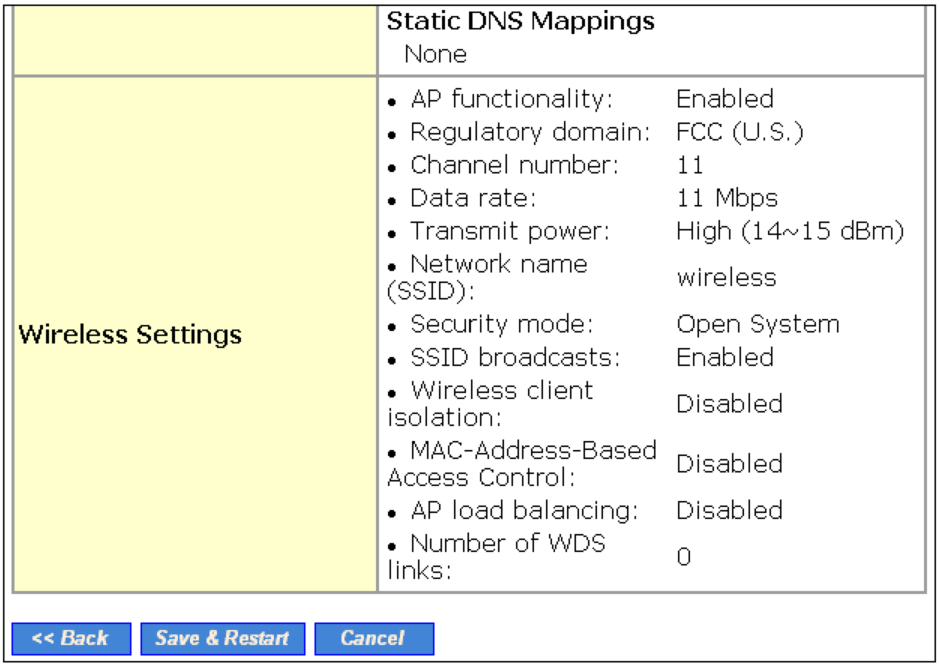
The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. The SSID of a wireless client computer and the SSID of the wireless access gateway must be identical for them to communicate with each other.

2.4.5. ConfigWizard Step 4: Reviewing and Applying Settings



Wireless Access Gateway Settings and Info	
Model	Access Gateway Adv
BIOS/Firmware Version	AGXP-ADM v1.10/1.1.3.824
Operational Mode	Gateway with a DHCP-based DSL/Cable connection
MAC Address (BSSID)	00-02-6F-01-C3-DF
System Up Time (hr:min:sec)	0:00:21
	WAN Connection Status: • Acquired IP: 192.168.168.221 • Acquired netmask: 255.255.255.0 • Acquired DNS server: 192.168.168.1 **WAN Interface** Obtain from a DHCP server • Trigger mode: Auto • Custom MAC address of WAN interface: Disabled

Fig. 11. Settings changes are highlighted in red.



	Static DNS Mappings None
Wireless Settings	• AP functionality: Enabled • Regulatory domain: FCC (U.S.) • Channel number: 11 • Data rate: 11 Mbps • Transmit power: High (14~15 dBm) • Network name (SSID): wireless • Security mode: Open System • SSID broadcasts: Enabled • Wireless client isolation: Disabled • MAC-Address-Based Access Control: Disabled • AP load balancing: Disabled • Number of WDS links: 0

Fig. 12. Settings review.

On the final page, you can review all the settings you have made. Changes are highlighted in red. If they are OK, click **Save & Restart** to apply the new settings. Or you can go back to previous pages to make modifications. Or you can click **Cancel** to leave the configuration process without any changes.

NOTE: About *7* seconds are needed for the gateway to complete its restart process.

2.4.6. Configuring User Authentication Settings

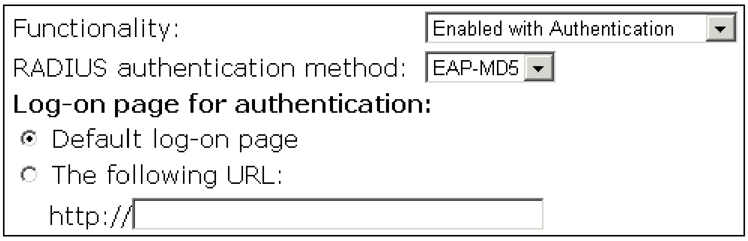
All editions of the WLAN hotspot access gateway support Web redirection-based user authentication. Furthermore, the *Wireless Advanced* edition of the access gateway, which has a built-in access point, supports IEEE 802.1x-based user authentication.

After the IP addressing settings have been set using ConfigWizard, you have to configure Web redirection settings and/or IEEE 802.1x settings for wireless user authentication.

NOTE: If both Web redirection and IEEE 802.1x are enabled, the authentication process is 2-phase. In the first phase, IEEE 802.1x is tried and in the second phase, Web redirection is tried. A user, who fails in the first phase or uses a computer that does not support IEEE 802.1x, is given a second chance. In this way, the wireless access gateway can serve both IEEE 802.1x-enabled and IEEE 802.1x-disabled wireless users.

2.4.6.1. Web Redirection

If you want to do Web redirection-based user authentication, go to the **Authentication, Web Redirection** section, and then enable the Web Redirection functionality by choosing **Enabled with Authentication** from the **Functionality** drop-down list and choose a **RADIUS authentication method** that is used by your RADIUS server. Click **Save** when finished.



Functionality: Enabled with Authentication

RADIUS authentication method: EAP-MD5

Log-on page for authentication:

● Default log-on page

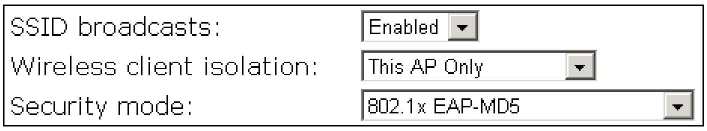
○ The following URL:

http://

Fig. 13. Web redirection settings.

TIP: There is an additional document on the accompanying CD-ROM, “Setting up a WLAN with Authentication Support Based on Web Redirection” which details how to set up a Web redirection-based authentication framework with a Windows 2000 server as the RADIUS server.

2.4.6.2. IEEE 802.1x



SSID broadcasts: Enabled

Wireless client isolation: This AP Only

Security mode: 802.1x EAP-MD5

Fig. 14. Changing security mode to an IEEE 802.1x option.

If you want to do IEEE 802.1x-based user authentication, go to the **IEEE 802.1x, Security** section, and then change the **Security mode** setting to an IEEE 802.1x-related option according to your needs. The advanced wireless access gateway supports IEEE 802.1x EAP-MD5 and EAP-TLS authentication methods. Click **Save** when finished.

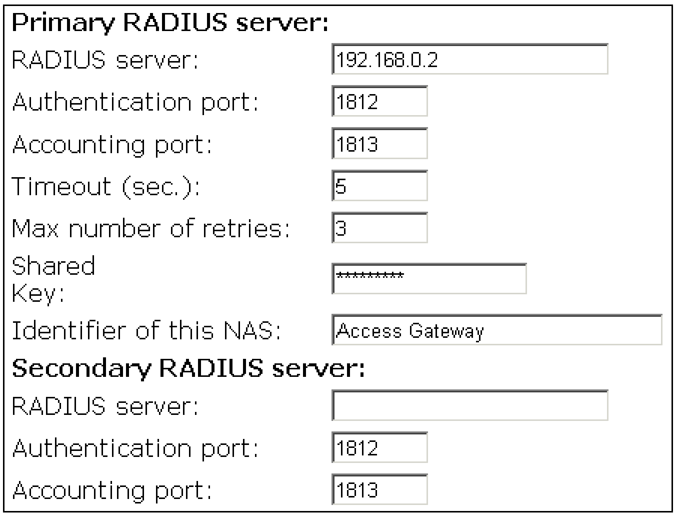
TIP: See the IEEE 802.1x-related white papers on the accompanying CD-ROM for more information about setting up an IEEE 802.1x-based authentication framework with a Windows 2000 server as the

RADIUS server.

2.4.7. Configuring RADIUS Settings

The RADIUS client on the WLAN hotspot access gateway works in conjunction with the Web redirection component and IEEE 802.1x component for wireless user authentication. The Web redirection and IEEE 802.1x components are responsible for acquiring user credential information, and the RADIUS client communicates with a back end RADIUS server using the user credential information.

Go to the **Authentication, RADIUS** section, and then configure the RADIUS settings. You have to configure at least **Authentication method**, **Primary RADIUS server**, **Shared key**, and **Identifier of this NAS settings**. And leave other settings to their default values. Click **Save & Restart** when finished.



Primary RADIUS server:	
RADIUS server:	192.168.0.2
Authentication port:	1812
Accounting port:	1813
Timeout (sec.):	5
Max number of retries:	3
Shared Key:	**********
Identifier of this NAS:	Access Gateway
Secondary RADIUS server:	
RADIUS server:	
Authentication port:	1812
Accounting port:	1813

Fig. 15. RADIUS settings.

NOTE: When configured for EAP authentication, the RADIUS server supports either EAP-TLS or EAP-MD5, but not both at the same time. As a result, not all combinations of EAP-MD5, EAP-TLS, PAP and CHAP authentication methods are available if both IEEE 802.1x and Web redirection are enabled. The following table shows the allowable IEEE 802.1x and Web redirection authentication modes on the *Wireless Advanced* edition of access gateway.

Table 1. Allowable authentication modes.

	IEEE 802.1x disabled	IEEE 802.1x EAP-MD5	IEEE 802.1x EAP-TLS
Web redirection disabled	■	■	■
Web redirection EAP-MD5	■	■	
Web redirection PAP	■	■	■
Web redirection CHAP	■	■	■

2.5. Deploying the WLAN Hotspot Access Gateway

After the settings have been configured, deploy the gateway to the field application environment. You have to connect AP(s), modem(s), and RADIUS server(s) to the gateway. The system configuration in Fig. 16 illustrates how to deploy the WLAN hotspot access gateway.

NOTE: The wireless model of WLAN hotspot access gateway has a built-in access point. If the RF coverage of the built-in access point is enough for your venue, no additional stand-alone access point is necessary.

In this configuration, one DSL/cable modem is connected to the WAN port (as WAN 1) of the gateway and another modem is connected to the LAN 1 port (as WAN 2) of the gateway. Two APs are connected to the LAN 2 port and LAN 3 port, respectively. Finally, a RADIUS server is connected to the LAN 4 port of the gateway. The gateway works together with the RADIUS server to decide whether a wireless client (the notebook computer or the PDA) is allowed to access the Internet through the broadband modems.

NOTE: Although the RADIUS server in this sample configuration is on the "LAN" side, in a real application, it can be on the "WAN" side, that is, on the Internet.

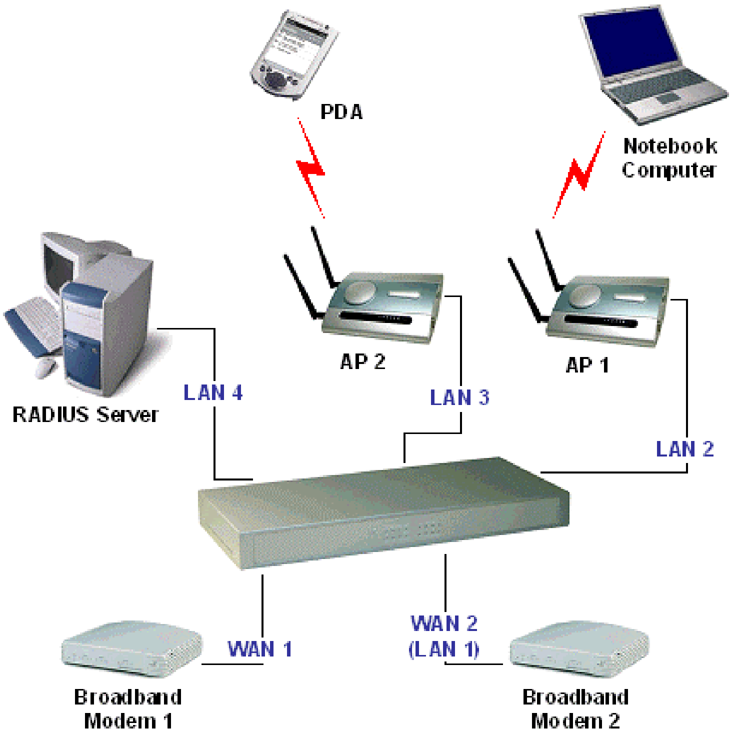


Fig. 16. Sample WLAN hotspot access gateway deployment.

2.6. Setting up Client Computers

Before a wireless user can access the Internet through the gateway, the wireless and TCP/IP settings of his/her computer or PDA must be configured adequately to match those of the gateway. In addition, if Web redirection or IEEE 802.1x EAP-MD5 authentication methods are used, *user name* and *password* information must be set up on the RADIUS server. On the other hand, if IEEE 802.1x EAP-TLS authentication method is used, a *digital certificate* must be installed on the computer or PDA and on the back end RADIUS server.

2.6.1. Configuring IEEE 802.11b-Related Settings

Before the TCP/IP networking system of a wireless client computer can communicate with other hosts, the underlying wireless link must be established between this wireless computer and a deployed AP or the wireless access gateway's built-in AP.

To establish a wireless link to an AP:

1. Launch the configuration/monitoring utility provided by the vendor of the installed WLAN NIC.

2. Use the utility to make appropriate *operating mode*, *SSID* and *WEP* settings.

NOTE: A wireless client computer must be in *infrastructure* mode, so that it can associate with a wireless access point.

NOTE: The SSID of the wireless client computer and the SSID of the deployed APs must be identical. Or, in case the **SSID broadcasts** capability of the deployed APs is enabled (by default), the SSID of the wireless client computer could be set to "any".

NOTE: Both the wireless client computer and the deployed APs must have the same WEP settings for them to communicate with each other. Therefore, unless IEEE 802.1x EAP-TLS, which supports dynamic WEP key distribution, is used, it's strongly suggested not to enable WEP functionality of the deployed APs for *hotspot* applications.

NOTE: If IEEE 802.1x authentication is to be used, see the IEEE 802.1x-related white papers on the accompanying CD-ROM for more information on setting up the wireless client computer.

2.6.2. Configuring TCP/IP-Related Settings

If a wireless user use a Windows computer, he/she can use **Windows Network Control Panel Applet** to change the TCP/IP settings of his/her computers, so that the IP addresses of the client computers and the IP address of the gateway are in the same IP subnet. If the access gateway is to be used in a hotspot, the client computers must be set to obtain IP addresses automatically by DHCP.

NOTE: Set the client computers to obtain IP addresses automatically by DHCP.

NOTE: Configure the client computers so that Web browsing is not through any Web Proxy servers; otherwise the Web redirection-based authentication will not work properly.

If a client computer is already set to obtain an IP address automatically, you can use the Windows-provided tool, **WinIPCfg.exe** (on Windows 9x) or **IPConfig.exe** (on Windows 2000), to re-obtain an IP address from the gateway. **WinIPCfg.exe** is a GUI program, and has command buttons for releasing the current IP address and re-obtaining an IP address. **IPConfig.exe** is a command-line program, and the **/release** option releases the current IP address and the **/renew** option triggers the Windows DHCP client subsystem to re-obtain an IP address.

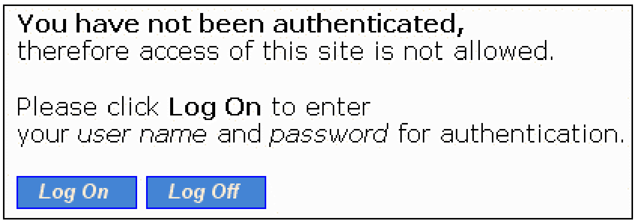
2.7. Confirming the Settings of the WLAN Hotspot Access Gateway and Client Computers

To make sure whether you have correctly set up the gateway for Web redirection-based authentication or not, follow the procedure below:

1. Establish a wireless link from the wireless client computer or PDA to an AP that is controlled by the gateway.

2. On the wireless client computer or PDA, run a Web browser, and then go to a Web site on the Internet, e.g., http://www.wi-fi.com.

3. Instead of showing the requested page, a log-on page is shown. Click **Log On** for authentication.

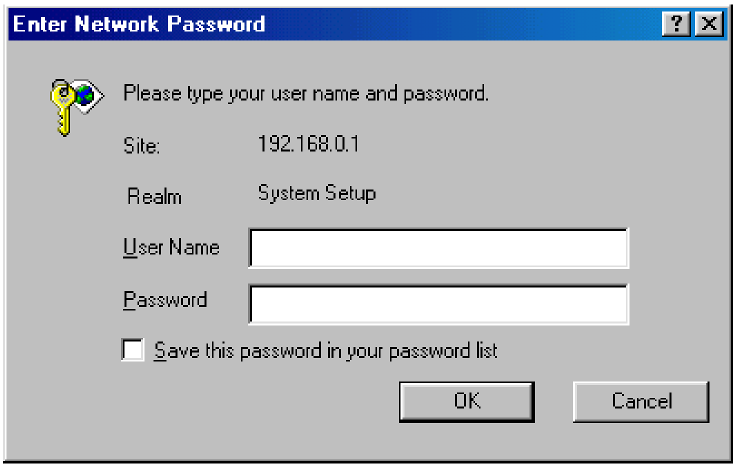


You have not been authenticated,
therefore access of this site is not allowed.

Please click **Log On** to enter
your *user name* and *password* for authentication.

Fig. 17. Log-on page.

4. Type a correct user name and password that has been registered on the RADIUS server.



Enter Network Password

Please type your user name and password.

Site: 192.168.0.1

Realm System Setup

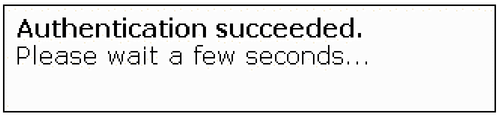
User Name

Password

□ Save this password in your password list

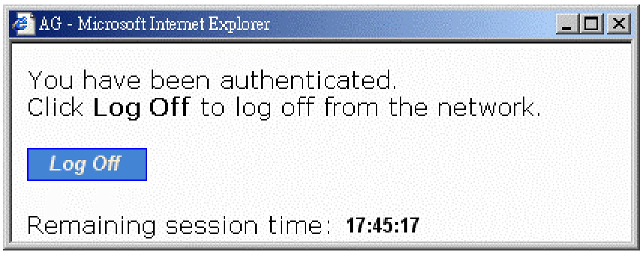
Fig. 18. User name and password for authentication.

5. If the user name and password are correct. Now you'll be brought to the original page you have requested after waiting for a few seconds. Meanwhile, a window for log-off and session status appears.



Authentication succeeded.
Please wait a few seconds...

Fig. 19. Authentication success.



AG - Microsoft Internet Explorer

You have been authenticated.
Click **Log Off** to log off from the network.

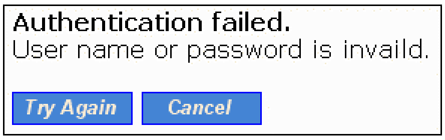
Remaining session time: **17:45:17**

Fig. 20. Log-off window.

6. Click **Log Off** within the log-off window to end the session.

NOTE: On a PDA such as Pocket PC, the log-off would not be shown. To log off from the network, go back to the Log-on page, and then click **Log Off** to end the session.

7. If the user name or password is invalid, you will be prompted to try again or cancel the authentication process.



Authentication failed.
User name or password is invaild.

Fig. 21. Authentication failure.

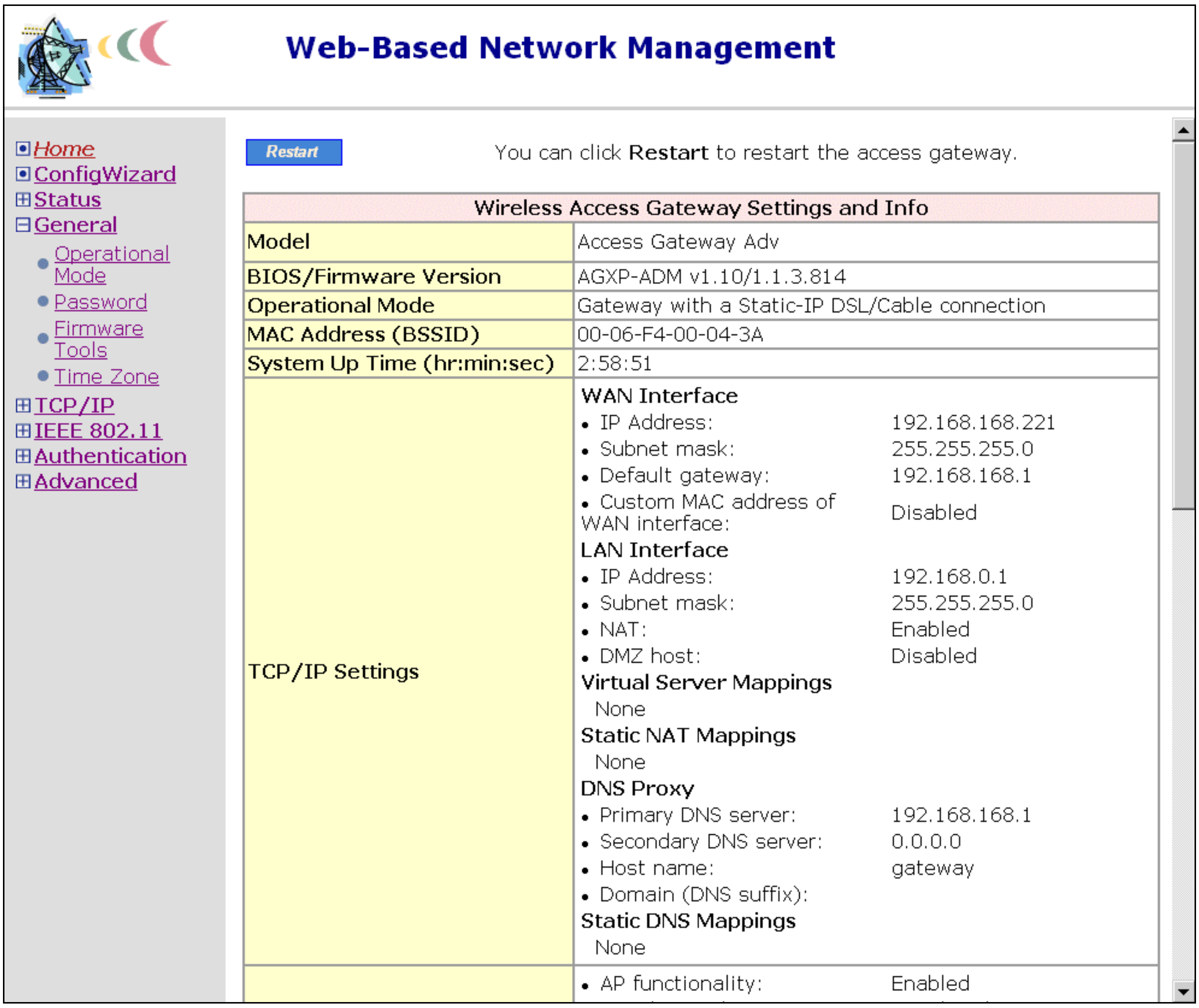
NOTE: If IEEE 802.1x capability of the *Wireless Advanced* edition of access gateway is enabled, the user of an IEEE 802.1x-compliant wireless client computer is authenticated by IEEE 802.1x rather than by Web redirection.

If you complete the above procedure without error, the gateway together with the RADIUS server has been correctly set up for Web redirection-based authentication.

3. Using Web-Based Network Manager

In this chapter, we'll explain each Web management page of the Web-based Network Manager in detail.

3.1. Overview



You can click **Restart** to restart the access gateway.

Wireless Access Gateway Settings and Info	
Model	Access Gateway Adv
BIOS/Firmware Version	AGXP-ADM v1.10/1.1.3.814
Operational Mode	Gateway with a Static-IP DSL/Cable connection
MAC Address (BSSID)	00-06-F4-00-04-3A
System Up Time (hr:min:sec)	2:58:51
TCP/IP Settings	WAN Interface • IP Address: 192.168.168.221 • Subnet mask: 255.255.255.0 • Default gateway: 192.168.168.1 • Custom MAC address of WAN interface: Disabled LAN Interface • IP Address: 192.168.0.1 • Subnet mask: 255.255.255.0 • NAT: Enabled • DMZ host: Disabled Virtual Server Mappings None Static NAT Mappings None DNS Proxy • Primary DNS server: 192.168.168.1 • Secondary DNS server: 0.0.0.0 • Host name: gateway • Domain (DNS suffix): Static DNS Mappings None
	• AP functionality: Enabled

Fig. 22. The Start page.

3.1.1. Menu Structure

The left side of the start page contains a menu for you to carry out commands. Here is a brief description of the hyperlinks on the menu:

- **Home.** For going back to the start page.
- **ConfigWizard.** For you to quickly set up the gateway.
- **Status.** Status information.
  - **Wireless Clients.** The status of the wireless clients currently associated with the wireless

access gateway's built-in AP.

  - **Authenticated Users.** The status and statistics of the RADIUS-authenticated users.
  - **DHCP Mappings.** Current IP-MAC address mappings.
  - **System Log.** Event log for what has happened inside the gateway.
  - **Session List.** Latest 50 incoming and 50 outgoing user traffic sessions processed by the NAT server component of the gateway.
  - **Managed LAN Devices.** The status of every LAN device managed by the gateway.

- **General.** Global operations.
  - **Operational Mode.** Operational mode of the gateway based on the type of the Internet connection provided by the ISP.
  - **Password.** For gaining rights to change or view the settings and status of the gateway.
  - **Firmware Tools.** For upgrading firmware, backing up and restoring configuration settings, and uploading a certificate file and a private file for SSL operations.
  - **Time Zone.** Time zone and SNTP (Simple Network Time Protocol) server settings.

- **TCP/IP.** TCP/IP-related settings.
  - **Addressing.** IP address settings for the gateway to work with TCP/IP, or user name and password provided by the ISP.
  - **DNS Proxy/Server.** DNS (Domain Name System) proxy and server settings.
  - **NAT Server.** Settings for the NAT (Network Address Translation) server on the gateway.
  - **DHCP Server.** Settings for the DHCP (Dynamic Host Configuration Protocol) server on the gateway.
  - **Dynamic DNS.** Settings for the dynamic DNS (DDNS) client on the gateway to communicate with a DDNS server for dynamic domain name registration.
  - **Bandwidth Management.** Settings for LAN-to-WAN traffic load balancing and client bandwidth control.
  - **PPTP Client.** Settings for PPTP- and Second Virtual LAN-based LAN device management.
  - **Zero Client Reconfiguration.** Settings for *zero client reconfiguration*. When this function is enabled, the gateway ignores IP, DNS, and/or SMTP (Simple Mail Transfer Protocol) settings of client computers.

- **IEEE 802.11.** IEEE 802.11b-related settings.
  - **Communication.** Communication settings for the IEEE 802.11b interface of the wireless access gateway to work properly with wireless clients.
  - **Security.** Security settings for authenticating wireless users by IEEE 802.1x and encrypt-

ing wireless data.

- **Authentication.** Wireless user authentication settings.
  - **Web Redirection.** Web redirection settings for how a wireless user's HTTP request is "redirected" for authentication.
  - **RADIUS.** RADIUS settings for communication with the primary and secondary RADIUS servers.
  - **Session Control.** Settings for controlling lifetimes of user authentication sessions.
  - **Auth Page Customization.** Settings for customizing the contents of *log-on*, *log-off*, *authentication success*, and *authentication failure* authentication pages.
- **Advanced.** Advanced settings of the gateway.
  - **Filters & Firewall.** Packet filtering and firewall settings for user access control and protection from hacker attacks from the Internet, respectively.
  - **Management.** Web-based management types, UPnP, and SNMP settings.
  - **Auto Recovery.** Settings for automatic recovery from lockup situations.
  - **LAN Device Management.** Settings for the gateway to know what LAN devices it has to manage.

3.1.2. Save, Save & Restart, and Cancel Commands

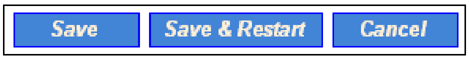
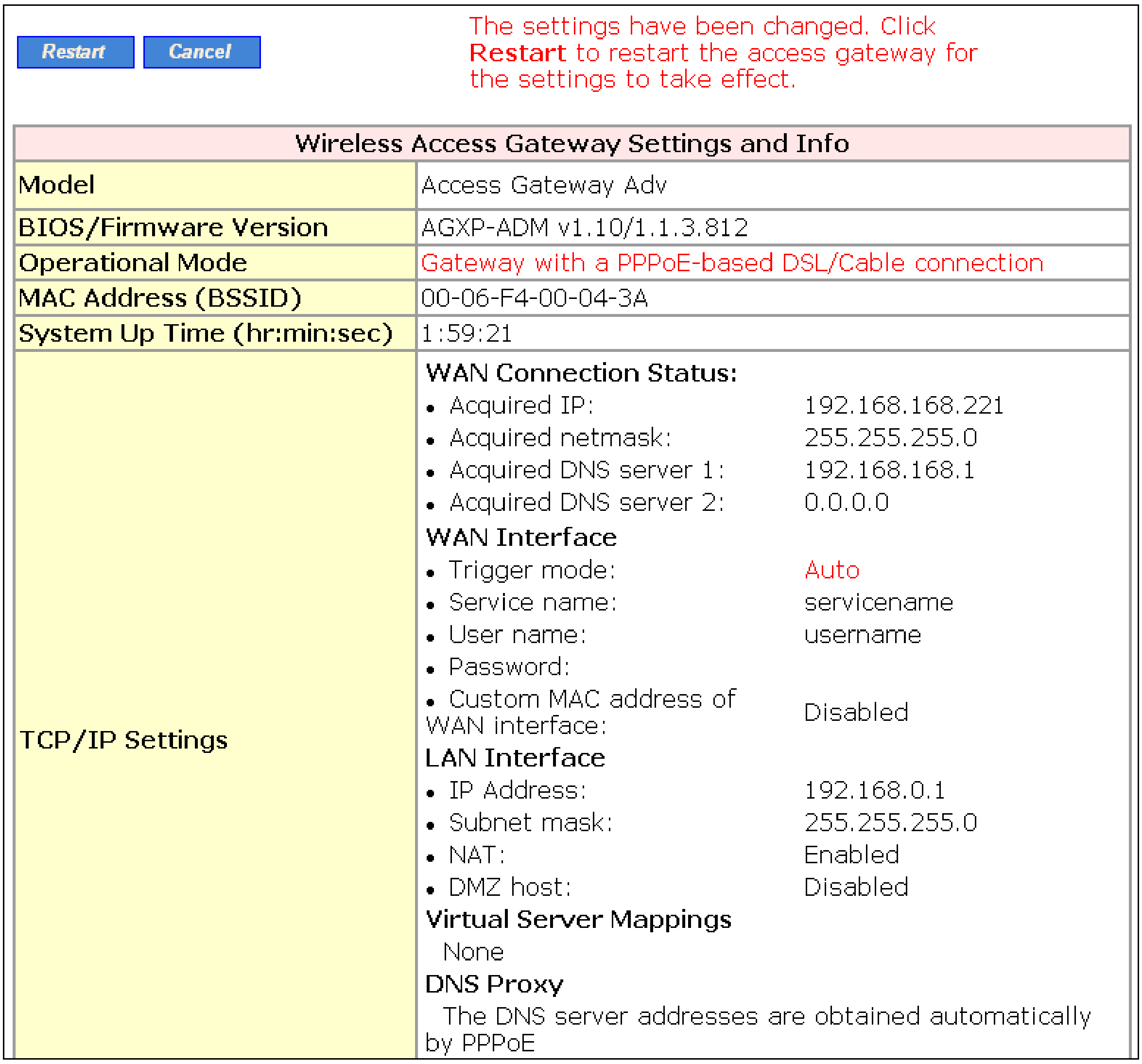


Fig. 23. Save, Save & Restart, and Cancel.

At the bottom of each page, there are up to three buttons—**Save**, **Save & Restart**, and **Cancel**. Clicking **Save** stores the settings changes to the memory of the gateway and brings you back to the start page. Clicking **Save& Restart** stores the settings changes to the memory of the gateway and restarts the gateway immediately for the settings changes to take effect. Clicking **Cancel** discards any settings changes and brings you back to the start page.

If you click **Save**, the start page will reflect the fact that the configuration settings have been changed by showing two buttons—**Restart** and **Cancel**. In addition, changes are highlighted in red. Clicking **Cancel** discards all the changes. Clicking **Restart** restarts the gateway for the settings changes to take effect.



The settings have been changed. Click **Restart** to restart the access gateway for the settings to take effect.

Wireless Access Gateway Settings and Info	
Model	Access Gateway Adv
BIOS/Firmware Version	AGXP-ADM v1.10/1.1.3.812
Operational Mode	Gateway with a PPPoE-based DSL/Cable connection
MAC Address (BSSID)	00-06-F4-00-04-3A
System Up Time (hr:min:sec)	1:59:21
TCP/IP Settings	WAN Connection Status: • Acquired IP: 192.168.168.221 • Acquired netmask: 255.255.255.0 • Acquired DNS server 1: 192.168.168.1 • Acquired DNS server 2: 0.0.0.0 WAN Interface • Trigger mode: Auto • Service name: servicename • User name: username • Password: • Custom MAC address of WAN interface: Disabled LAN Interface • IP Address: 192.168.0.1 • Subnet mask: 255.255.255.0 • NAT: Enabled • DMZ host: Disabled Virtual Server Mappings None DNS Proxy The DNS server addresses are obtained automatically by PPPoE

Fig. 24. Settings have been changed.

3.1.3. Home and Refresh Commands

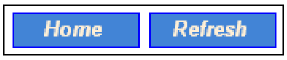
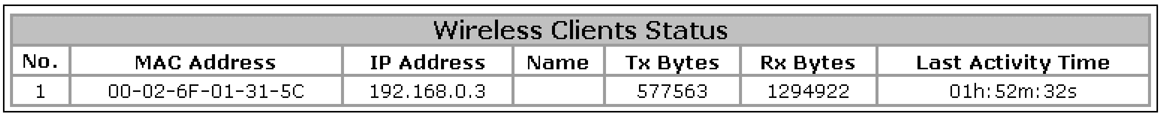


Fig. 25. Home and Refresh.

At the bottom of each status page that shows read-only information, there are two buttons—**Home** and **Refresh**. Clicking **Home** brings you back to the start page. Clicking **Refresh** updates the shown status information.

3.2. Viewing Status

3.2.1. Associated Wireless Clients



Wireless Clients Status

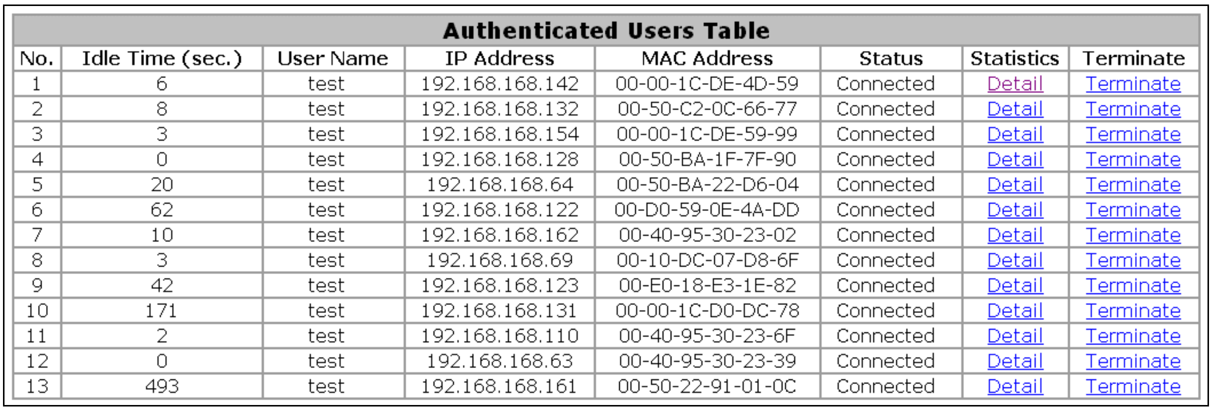
No.	MAC Address	IP Address	Name	Tx Bytes	Rx Bytes	Last Activity Time
1	00-02-6F-01-31-5C	192.168.0.3		577563	1294922	01h:52m:32s

Fig. 26. Status of associated wireless clients.

On this page, the status information of each associated client, including its MAC address, IP address, user name (if the client has been IEEE 802.1x authenticated), number of bytes it has sent, number of bytes it has received, and the time of its last activity, is shown.

NOTE: The information on this page is presented from the perspective of the wireless access gateway's built-in AP. For a wired edition of access gateway, this page is missing.

3.2.2. Authenticated Users



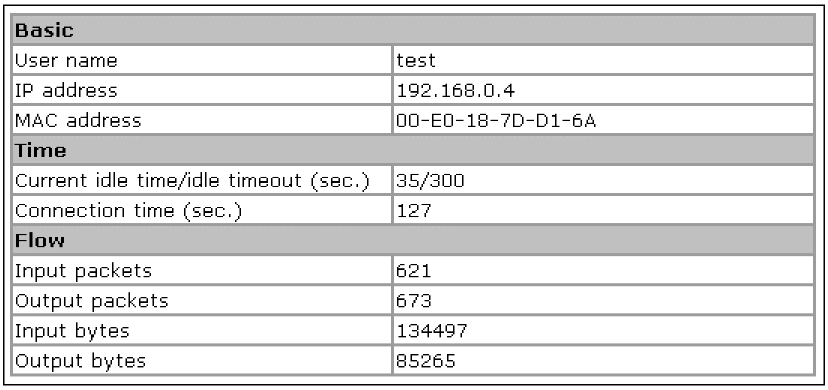
Authenticated Users Table

No.	Idle Time (sec.)	User Name	IP Address	MAC Address	Status	Statistics	Terminate
1	6	test	192.168.168.142	00-00-1C-DE-4D-59	Connected	Detail	Terminate
2	8	test	192.168.168.132	00-50-C2-0C-66-77	Connected	Detail	Terminate
3	3	test	192.168.168.154	00-00-1C-DE-59-99	Connected	Detail	Terminate
4	0	test	192.168.168.128	00-50-BA-1F-7F-90	Connected	Detail	Terminate
5	20	test	192.168.168.64	00-50-BA-22-D6-04	Connected	Detail	Terminate
6	62	test	192.168.168.122	00-D0-59-0E-4A-DD	Connected	Detail	Terminate
7	10	test	192.168.168.162	00-40-95-30-23-02	Connected	Detail	Terminate
8	3	test	192.168.168.69	00-10-DC-07-D8-6F	Connected	Detail	Terminate
9	42	test	192.168.168.123	00-E0-18-E3-1E-82	Connected	Detail	Terminate
10	171	test	192.168.168.131	00-00-1C-D0-DC-78	Connected	Detail	Terminate
11	2	test	192.168.168.110	00-40-95-30-23-6F	Connected	Detail	Terminate
12	0	test	192.168.168.63	00-40-95-30-23-39	Connected	Detail	Terminate
13	493	test	192.168.168.161	00-50-22-91-01-0C	Connected	Detail	Terminate

Fig. 27. Authenticated users.

On this page, the status information of each RADIUS-authenticated user, including its current idle time, user name, IP address, MAC address, and status, is shown. In addition, you can click the **Detail** link in the **Statistics** column to see more detailed statistics information, such as **Input packets**, **Output packets**, **Input bytes**, and **Output bytes**.

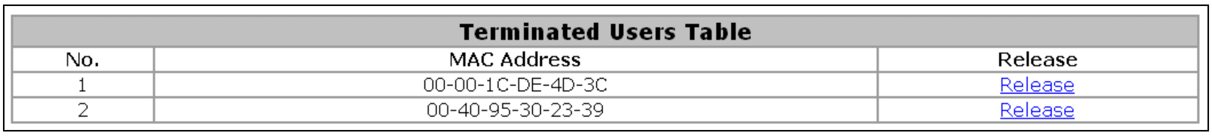
NOTE: The information on this page is presented from the perspective of the access gateway's RADIUS client. Every edition of access gateway has this page.



Basic	
User name	test
IP address	192.168.0.4
MAC address	00-E0-18-7D-D1-6A
Time	
Current idle time/idle timeout (sec.)	35/300
Connection time (sec.)	127
Flow	
Input packets	621
Output packets	673
Input bytes	134497
Output bytes	85265

Fig. 28. Authenticated RADIUS user detailed information.

Any authenticated user can be terminated by clicking the corresponding **Terminate** link so that this user is blocked from using networking services provided by the gateway. A terminated user is moved to the **Terminated Users Table**. Clicking the corresponding **Release** link puts a terminated user back into authenticated state.

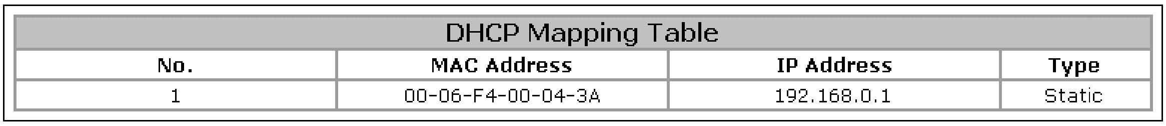


Terminated Users Table

No.	MAC Address	Release
1	00-00-1C-DE-4D-3C	Release
2	00-40-95-30-23-39	Release

Fig. 29. Terminated users.

3.2.3. Current DHCP Mappings



DHCP Mapping Table

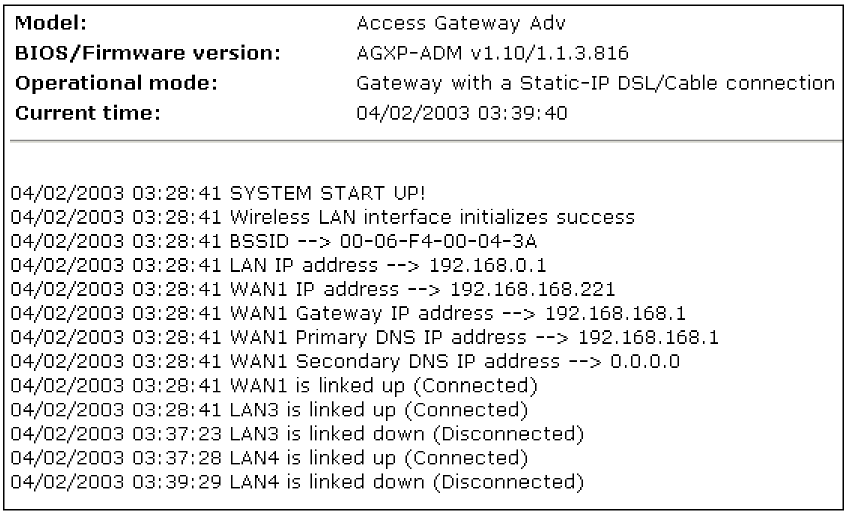
No.	MAC Address	IP Address	Type
1	00-06-F4-00-04-3A	192.168.0.1	Static

Fig. 30. Current DHCP mappings.

On this page, all the current *static* or *dynamic* DHCP mappings are shown. A DHCP mapping is a correspondence relationship between an IP address assigned by the DHCP server and a computer or device that obtains the IP address. A computer or device that acts as a DHCP client is identified by its MAC address.

A static mapping indicates that the DHCP client always obtains the specified IP address from the DHCP server. You can set static DHCP mappings in the **Static DHCP Mappings** section of the **DHCP Server** configuration page (see Section 0). A dynamic mapping indicates that the DHCP server chooses an IP address from the IP address pool specified by the **First allocateable IP address** and **Allocateable IP address count** settings on the **DHCP Server** configuration page.

3.2.4. System Log



Model: Access Gateway Adv

BIOS/Firmware version: AGXP-ADM v1.10/1.1.3.816

Operational mode: Gateway with a Static-IP DSL/Cable connection

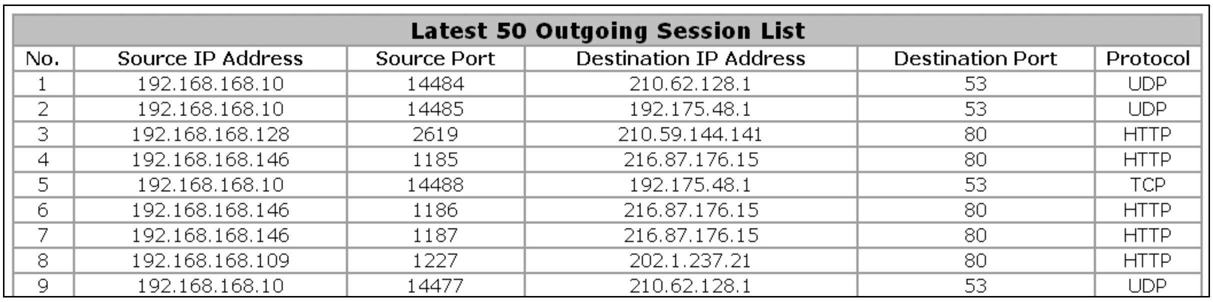
Current time: 04/02/2003 03:39:40

```
04/02/2003 03:28:41 SYSTEM START UP!
04/02/2003 03:28:41 Wireless LAN interface initializes success
04/02/2003 03:28:41 BSSID --> 00-06-F4-00-04-3A
04/02/2003 03:28:41 LAN IP address --> 192.168.0.1
04/02/2003 03:28:41 WAN1 IP address --> 192.168.168.221
04/02/2003 03:28:41 WAN1 Gateway IP address --> 192.168.168.1
04/02/2003 03:28:41 WAN1 Primary DNS IP address --> 192.168.168.1
04/02/2003 03:28:41 WAN1 Secondary DNS IP address --> 0.0.0.0
04/02/2003 03:28:41 WAN1 is linked up (Connected)
04/02/2003 03:28:41 LAN3 is linked up (Connected)
04/02/2003 03:37:23 LAN3 is linked down (Disconnected)
04/02/2003 03:37:28 LAN4 is linked up (Connected)
04/02/2003 03:39:29 LAN4 is linked down (Disconnected)
```

Fig. 31. System log.

The system log shows events happening inside the gateway since the gateway starts up. The logged information is useful for troubleshooting purposes. For example, if the password configured for PPPoE is incorrect, this error can be easily spotted by inspecting the system log. The system events are divided into several categories, and you can select which categories of events to log. See Section 3.7.2.3 for more information.

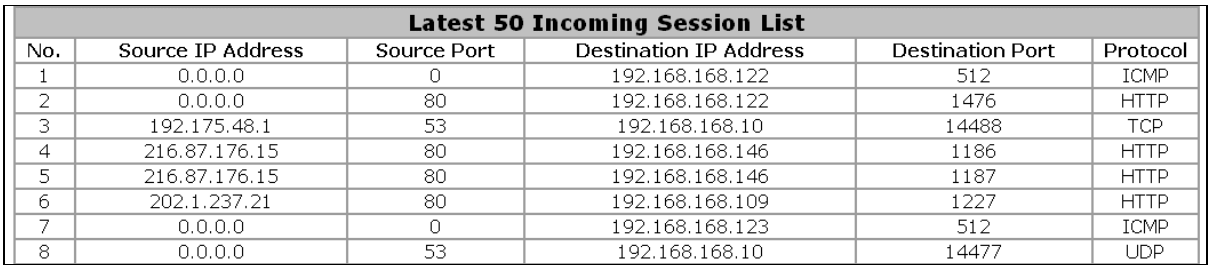
3.2.5. Outgoing and Incoming User Traffic Sessions



Latest 50 Outgoing Session List

No.	Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol
1	192.168.168.10	14484	210.62.128.1	53	UDP
2	192.168.168.10	14485	192.175.48.1	53	UDP
3	192.168.168.128	2619	210.59.144.141	80	HTTP
4	192.168.168.146	1185	216.87.176.15	80	HTTP
5	192.168.168.10	14488	192.175.48.1	53	TCP
6	192.168.168.146	1186	216.87.176.15	80	HTTP
7	192.168.168.146	1187	216.87.176.15	80	HTTP
8	192.168.168.109	1227	202.1.237.21	80	HTTP
9	192.168.168.10	14477	210.62.128.1	53	UDP

Fig. 32. Latest outgoing user traffic sessions.



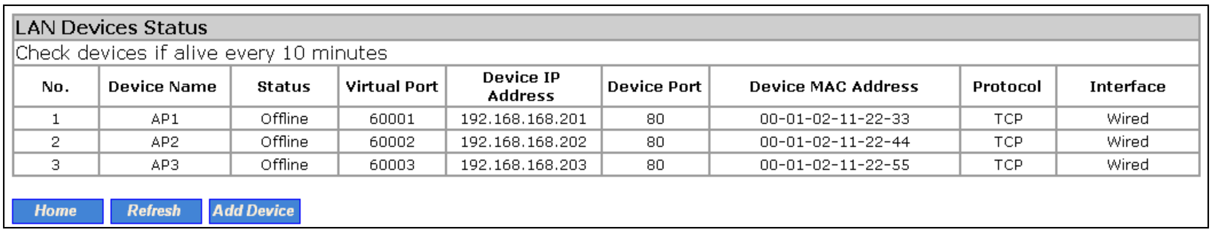
Latest 50 Incoming Session List

No.	Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol
1	0.0.0.0	0	192.168.168.122	512	ICMP
2	0.0.0.0	80	192.168.168.122	1476	HTTP
3	192.175.48.1	53	192.168.168.10	14488	TCP
4	216.87.176.15	80	192.168.168.146	1186	HTTP
5	216.87.176.15	80	192.168.168.146	1187	HTTP
6	202.1.237.21	80	192.168.168.109	1227	HTTP
7	0.0.0.0	0	192.168.168.123	512	ICMP
8	0.0.0.0	53	192.168.168.10	14477	UDP

Fig. 33. Latest incoming user traffic sessions.

On this page, latest 50 outgoing and 50 incoming user traffic sessions are shown for monitoring network activity.

3.2.6. Managed LAN Devices



LAN Devices Status

Check devices if alive every 10 minutes

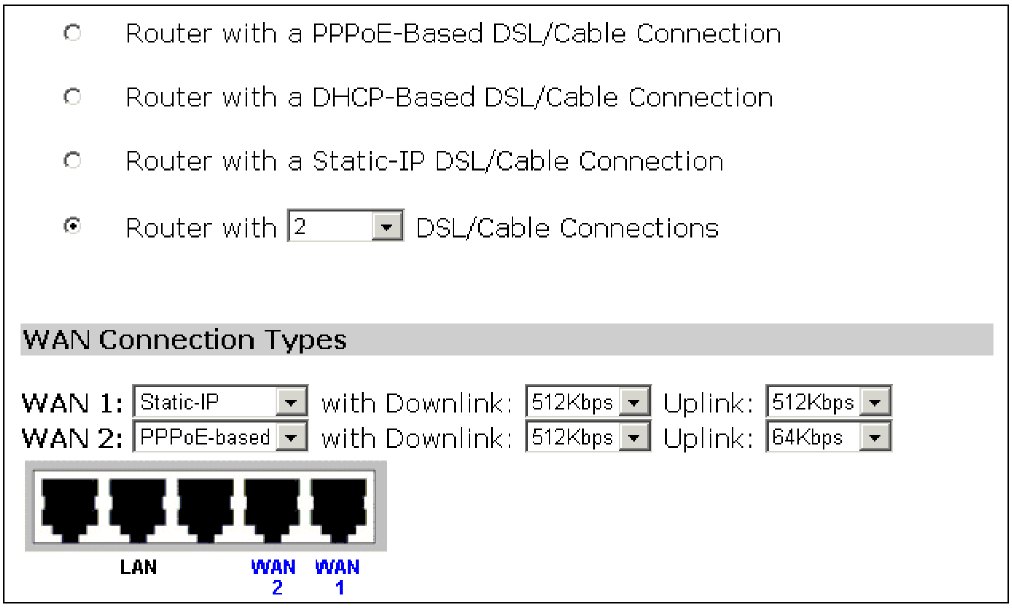
No.	Device Name	Status	Virtual Port	Device IP Address	Device Port	Device MAC Address	Protocol	Interface
1	AP1	Offline	60001	192.168.168.201	80	00-01-02-11-22-33	TCP	Wired
2	AP2	Offline	60002	192.168.168.202	80	00-01-02-11-22-44	TCP	Wired
3	AP3	Offline	60003	192.168.168.203	80	00-01-02-11-22-55	TCP	Wired

Fig. 34. Managed LAN devices.

On this page, the status of every managed LAN device is shown. The *Offline* status indicates a non-working device while the *Online* status indicates a working device. The **Add Device** button serves as a shortcut to the **Advanced, LAN Device Management** configuration page, on which you can specify which devices to manage. See Section 3.7.3 for more information.

3.3. General Operations

3.3.1. Specifying Operational Mode



○ Router with a PPPoE-Based DSL/Cable Connection

○ Router with a DHCP-Based DSL/Cable Connection

○ Router with a Static-IP DSL/Cable Connection

● Router with 2 DSL/Cable Connections

WAN Connection Types

WAN 1: Static-IP with Downlink: 512Kbps Uplink: 512Kbps

WAN 2: PPPoE-based with Downlink: 512Kbps Uplink: 64Kbps

Fig. 35. Operational modes.

On this page, you can specify the operational mode for the gateway. Currently, *5* modes are available:

- **Gateway with a PPPoE-based DSL/Cable Connection.** In this mode, the gateway assumes that a DSL or cable modem is connected to its Ethernet WAN interface. The client computers can therefore share this DSL/cable-based Internet connection by the NAT server functionality. The IP address of the Ethernet WAN interface is obtained automatically by PPPoE from the ISP.

- **Gateway with a DHCP-based DSL/Cable Connection.** In this mode, the gateway assumes that a DSL or cable modem is connected to its Ethernet WAN interface. The client computers can therefore share this DSL/cable-based Internet connection by the NAT server functionality. The IP address of the Ethernet WAN interface is obtained automatically by DHCP from the ISP.

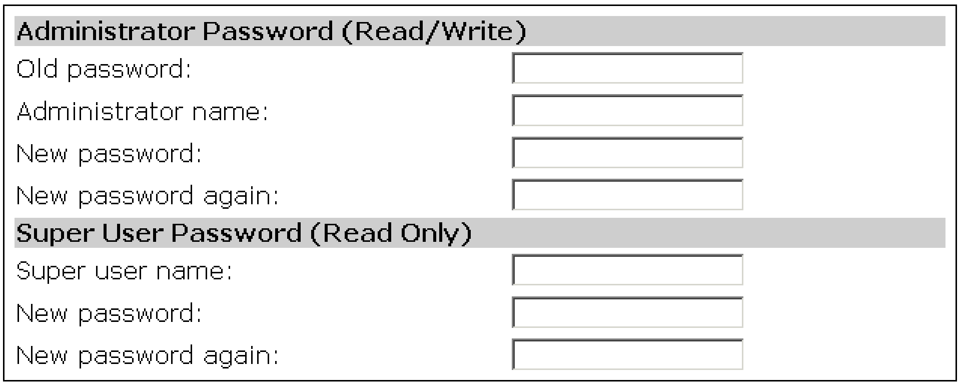
- **Gateway with a Static-IP DSL/Cable Connection.** In this mode, the gateway assumes that a DSL or cable modem is connected to its Ethernet WAN interface. The client computers can therefore share this DSL/cable-based Internet connection by the NAT server functionality. The IP address of the Ethernet WAN interface must be manually set.

- **Gateway with *n* DSL/Cable Connections.** In this mode, the gateway can support up to 4 (*n* = 2 to 4) DSL/cable-based Internet connections. The client computers can share the bandwidth of these Internet connections by the NAT server functionality. Since there are multiple Internet connections, total throughput is increased. The specified downlink and uplink data rates affect the load-balancing engine of the gateway.

TIP: After you have selected the operational mode of the gateway, go to the **TCP/IP, Addressing** section of the management UI (see Section 3.4.1) to configure the addressing settings of the WAN and LAN interfaces.

NOTE: Since the WAN load-balancing algorithm is based on the "TCP session" rather than on the "packet," a TCP session is allocated to a WAN connection at session initialization time. As a result, if there is only one client, no throughput improvement will be perceived even if there are several WAN connections. WAN load balancing is for multiple clients to share the multiple WAN connections. All the TCP sessions from the clients are intelligently distributed to the WAN connections by the built-in NAT server.

3.3.2. Changing Password



Administrator Password (Read/Write)

Old password:

Administrator name:

New password:

New password again:

Super User Password (Read Only)

Super user name:

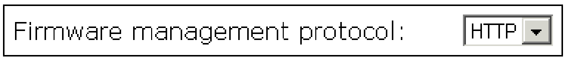
New password:

New password again:

Fig. 36. Password.

On this page, you could change the user name and password of the *administrator* and/or of the *super user*. The administrator can view and modify the configuration of the access gateway while the super user can only view the configuration. The new password must be typed twice for confirmation.

3.3.3. Managing Firmware



Firmware management protocol: HTTP

Fig. 37. Firmware management protocol setting.

Firmware management operations for the access gateway include *firmware upgrade*, *configuration* *backup*, *configuration restore*, and *configuration reset*. Firmware upgrade, configuration backup, and configuration restore can be achieved via HTTP or TFTP. The HTTP-based way is suggested because it's more user friendly. However, due to different behavior of different Web browser versions, HTTP-based firmware management operations may not work properly with some Web browsers. If you cannot successfully perform HTTP-based firmware management operations with your Web browser, try the TFTP-based way.

3.3.3.1. Upgrading Firmware by HTTP

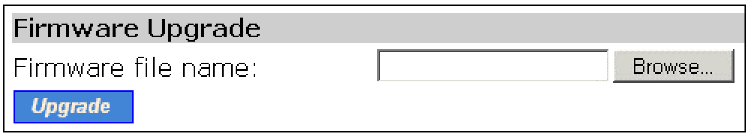


Fig. 38. Firmware upgrade by HTTP.

To upgrade firmware of the access gateway by HTTP:

1. Click **Browse** and then select a correct firmware **.bin** file. The firmware file path will be shown in the **Firmware file name** text box.

2. Click **Upgrade** to begin the upgrade process.

3.3.3.2. Backing up and Restoring Configuration Settings by HTTP

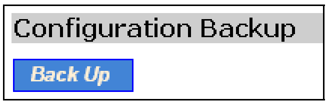


Fig. 39. Firmware backup by HTTP.

To back up configuration of the access gateway by HTTP:

1. Click **Back Up**.

2. You'll be prompted to open or save the configuration file. Click **Save**.

3. The configuration file is named by the gateway's MAC address. For example, if the gateway's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex". Don't change the configuration file name in the **Save As** dialog box. Select a folder in which the configuration file is to be stored. And then, click **Save**.

NOTE: The procedure may be a little different with different Web browsers.

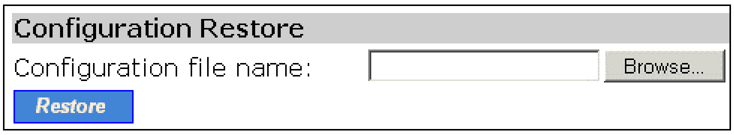


Fig. 40. Configuration restore by HTTP.

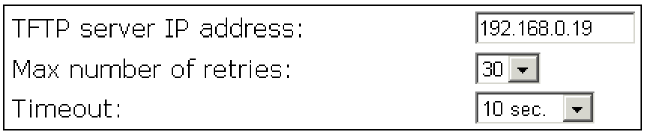
To restore configuration of the access gateway by HTTP:

1. Click **Browse** and then select a correct configuration **.hex** file. You have to make sure the file

name is the access gateway's MAC address. The firmware file path will be shown in the **Firmware file name** text box.

2. Click **Restore** to upload the configuration file to the access gateway.

3.3.3.3. Upgrading Firmware by TFTP



TFTP server IP address: 192.168.0.19

Max number of retries: 30

Timeout: 10 sec.

Fig. 41. TFTP server settings.

When use TFTP as the firmware management protocol, you can configure settings for the access gateway's TFTP client to communicate with a TFTP server. If the TFTP client does not get a response from the TFTP server within a period specified by the **Timeout** setting, it will resend the previous request. The **Max number of retries** setting specifies the maximal number of resend before the TFTP client stops communicating with the TFTP server.

Within the folder "**Utilities**" on the companion CD-ROM disk, we offered a TFTP server program (**TftpSrvr.exe**) for firmware upgrade. Run this program on the computer that is to serve as a TFTP server.

Firmware Upgrade

Fig. 42. Firmware upgrade by TFTP.

To upgrade firmware of the access gateway by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the upgrade process.

2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.

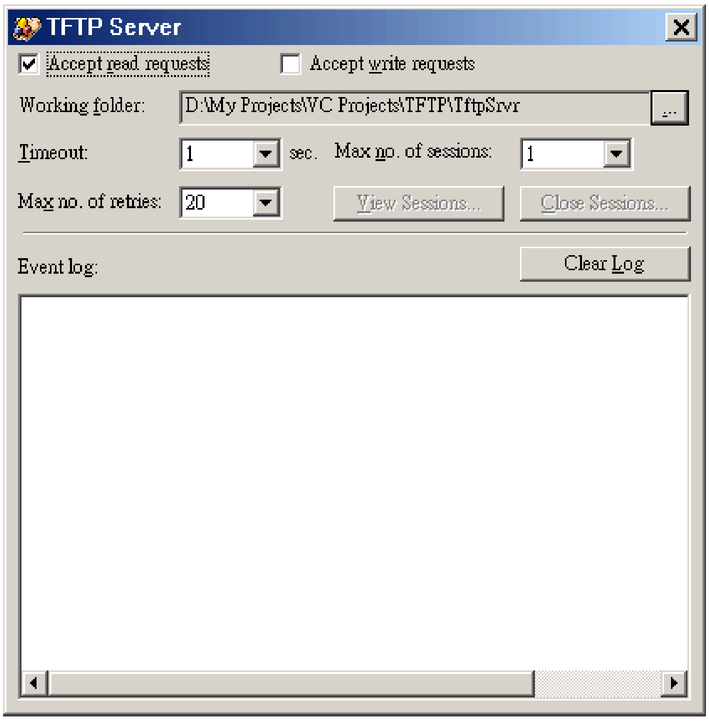
3. Configure IP address of the computer so that the gateway and the computer are in the same IP subnet.

4. On the computer, run the TFTP Server utility. And specify the folder in which the firmware files reside.

5. On the computer, run a Web browser and click the **General, Firmware Upgrade** hyperlink.

6. Specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.

7. Trigger the firmware upgrade process by clicking **Upgrade**.



☑ Accept read requests □ Accept write requests

Working folder: D:\My Projects\VC Projects\TFTP\TftpSrvr

Timeout: 1 sec. Max no. of sessions: 1

Max no. of retries: 20

Event log:

Fig. 43. TFTP Server.

NOTE: After the dialog box of the TFTP server program appears, be sure to specify the working folder within which the downloaded firmware files reside.

NOTE: Make sure the **Accept read requests** check box of TFTP Server is selected.

NOTE: The LAN IP address of the gateway and the IP address of the TFTP server must be in the same IP subnet for TFTP to work.

NOTE: Due to the unreliable nature of wireless media, it's highly recommended that the TFTP server and the to-be-upgraded wireless access gateway be connected by Ethernet, and on the same LAN, so that the upgrade process would be smooth.

NOTE: After the firmware is upgraded, be sure to delete the contents of the Web browser cache, so that the Web management pages can be shown correctly.

NOTE: A failed upgrade may corrupt the firmware and make the gateway unstartable. When this occurs, call for technical support.

TIP: The firmware of a *deployed* access gateway can also be upgraded remotely from the Internet. In this case, you must have configured the gateway to be remotely manageable (see Section 3.6.1.1) and adjust the **Timeout** and **Max no. of retries** settings of TFTP Server for remote TFTP upgrade to succeed.

3.3.3.4. Backing up and Restoring Configuration Settings by TFTP

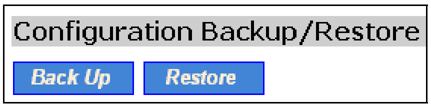


Fig. 44. Configuration backup/restore.

To back up configuration of the access gateway by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the backup process.

2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.

3. Configure the IP address of the computer so that the computer and the gateway are in the same IP subnet.

4. On the computer, run the TFTP Server utility. Select the **Accept write requests** check box, and specify the folder to which the configuration settings of the gateway will be saved.

5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.

6. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.

7. Trigger the backup process by clicking **Back Up**. The gateway's configuration settings will be saved as "**AaBbCcDdEeFf.hex**" by the TFTP server, where "AaBbCcDdEeFf" is the gateway's MAC address. For example, if the gateway's MAC address is 00-01-02-33-44-55, the configuration backup file will be "000102334455.hex".

NOTE: Remember to select the **Accept write requests** check box of TFTP Server.

To restore configuration of the access gateway by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the restoring process.

2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.

3. Configure the IP address of the computer so that the computer and the gateway are in the same IP subnet.

4. On the computer, run the TFTP Server utility. And specify the folder in which the configuration backup file resides. A configuration backup file is named by the gateway's MAC address. For example, if the gateway's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex".

5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.

6. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.

7. Trigger the restoring process by clicking **Restore**. The gateway will then download the configuration backup file from the TFTP server.

NOTE: Make sure the file is a valid configuration backup file for the access gateway.

TIP: The configuration of a *deployed* access gateway can also be backed up or restored remotely from the Internet. In this case, you must have configured the gateway to be remotely manageable (see Section 3.7.2.1) and adjust the **Timeout** and **Max no. of retries** settings of TFTP Server for remote TFTP configuration backup/restore to succeed.

3.3.3.5. Resetting Configuration to Factory Defaults

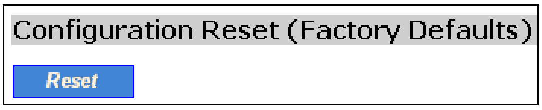
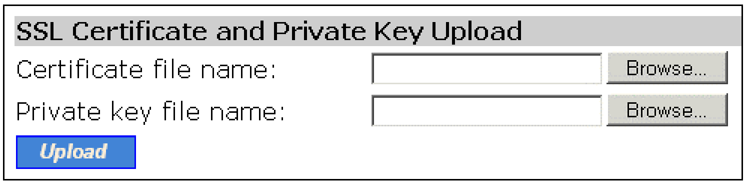

Configuration Reset (Factory Defaults)

Fig. 45. Configuration reset.

Clicking the **Reset** button resets the device configuration to factory defaults.

WARNING: Think twice before clicking the **Reset** button. You'll lose all your current configuration settings.

3.3.3.6. Uploading a Certificate and a Private Key File


SSL Certificate and Private Key Upload

Certificate file name:

Private key file name:

Fig. 46. SSL Certificate and private key upload.

The gateway can use SSL (Secure Socket Layer) to encrypt username and password information transmitted during a Web redirection-based authentication process. The gateway is equipped with a default X.509 certificate and private key for this purpose. As an alternative, you can use a certificate and private key issued by a third party CA (Certificate Authority) that you trust.

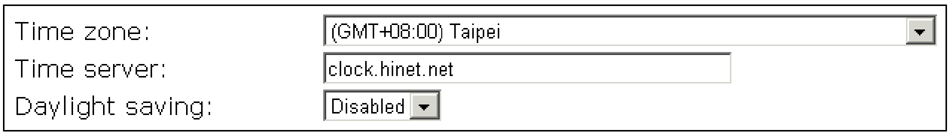
To upload a certificate file and private key file to the access gateway:

1. Click **Browse** next to the **Certificate file name** text box and select a certificate file. The certificate file path will be shown in the **Certificate file name** text box.

2. Click **Browse** next to the **Private key file name** text box and select the private key file that is associated with the certificate file. The private key file path will be shown in the **Private key file name** text box.

3. Click **Upload** to upload the certificate file and private key file to the access gateway.

3.3.4. Setting Time Zone


Time zone: (GMT+08:00) Taipei

Time server: clock.hinet.net

Daylight saving: Disabled

Fig. 47. Time zone and time server settings.

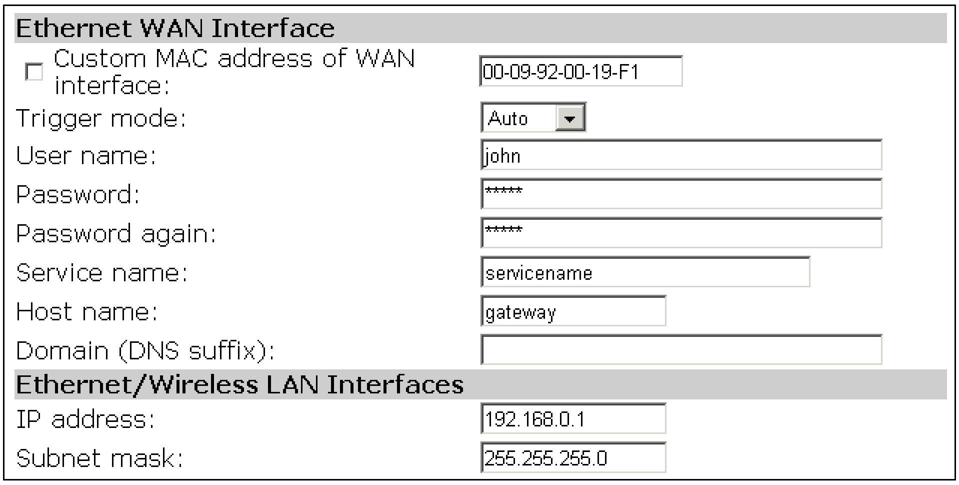
The gateway supports absolute system time by querying the SNTP (Simple Network Time Protocol) time server specified by the **Time server** setting. And you should specify the **Time zone** according to where you are. If your location adopts Daylight Saving Time, enable **Daylight saving**.

3.4. Configuring TCP/IP Related Settings

3.4.1. Addressing

The addressing settings depend on the operational mode of the gateway. Each operational mode requires different addressing settings.

3.4.1.1. Gateway with a PPPoE-Based DSL/Cable Connection



Ethernet WAN Interface	
□ Custom MAC address of WAN interface:	00-09-92-00-19-F1
Trigger mode:	Auto
User name:	john
Password:	*****
Password again:	*****
Service name:	servicename
Host name:	gateway
Domain (DNS suffix):	
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.0.1
Subnet mask:	255.255.255.0

Fig. 48. TCP/IP settings for **Gateway with a PPPoE-Based DSL/Cable Connection** mode.

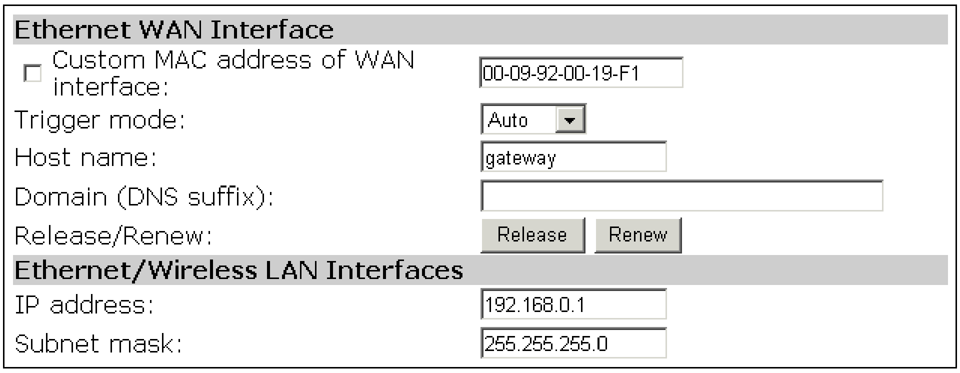
If the gateway was set to be in **Gateway with a PPPoE-Based DSL/Cable Connection** mode, two IP addresses are needed—one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained automatically by PPPoE from the ISP. Consult your ISP for the correct **User name**, **Password**, and **Service name** settings.

The **Trigger mode** setting specifies the way a PPPoE connection is established. Your PPPoE connection can be established and torn down *manually* (**Manual**) by clicking the **Connect** and **Disconnect** buttons on the Start page, respectively. Or you can choose to let the device *automatically* (**Auto**) establish a PPPoE connection at bootup time. In **Auto** mode, if the connection is disrupted, the device will try to re-establish the broken connection automatically.

Custom MAC Address of WAN Interface enables you to change the MAC address of the Ethernet WAN interface. Therefore, if the ISP-provided DSL or cable modem works only with the ISP-provided Ethernet card for a computer, the WAN interface of the gateway can mimic the ISP-provided Ethernet card by changing its MAC address to the Ethernet card's MAC address.

3.4.1.2. Gateway with a DHCP-Based DSL/Cable Connection


Ethernet WAN Interface

□ Custom MAC address of WAN interface: 00-09-92-00-19-F1

Trigger mode: Auto

Host name: gateway

Domain (DNS suffix):

Release/Renew:

Ethernet/Wireless LAN Interfaces

IP address: 192.168.0.1

Subnet mask: 255.255.255.0

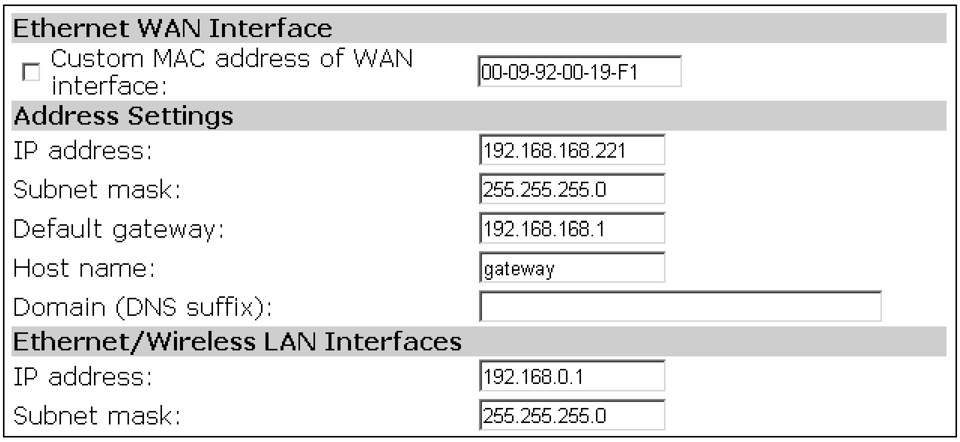
Fig. 49. TCP/IP settings for **Gateway with a DHCP-Based DSL/Cable Connection** mode.

If the gateway was set to be in **Gateway with a DHCP-Based DSL/Cable Connection** mode, two IP addresses are needed—one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained by DHCP from the ISP. The **Trigger mode** setting affects the behavior of the DHCP client of the gateway. In **Auto** mode, you don't have to worry about the DHCP process; the device takes care of everything. In **Manual** mode, there are two buttons on the Start page for you to manually release an obtained IP address (**Release**) and re-obtain a new one from a DHCP server (**Renew**).

Custom MAC Address of WAN Interface enables you to change the MAC address of the Ethernet WAN interface. Therefore, if the ISP-provided DSL or cable modem works only with the ISP-provided Ethernet card for a computer, the WAN interface of the gateway can mimic the ISP-provided Ethernet card by changing its MAC address to the Ethernet card's MAC address.

3.4.1.3. Gateway with a Static-IP DSL/Cable Connection


Ethernet WAN Interface

□ Custom MAC address of WAN interface: 00-09-92-00-19-F1

Address Settings

IP address: 192.168.168.221

Subnet mask: 255.255.255.0

Default gateway: 192.168.168.1

Host name: gateway

Domain (DNS suffix):

Ethernet/Wireless LAN Interfaces

IP address: 192.168.0.1

Subnet mask: 255.255.255.0

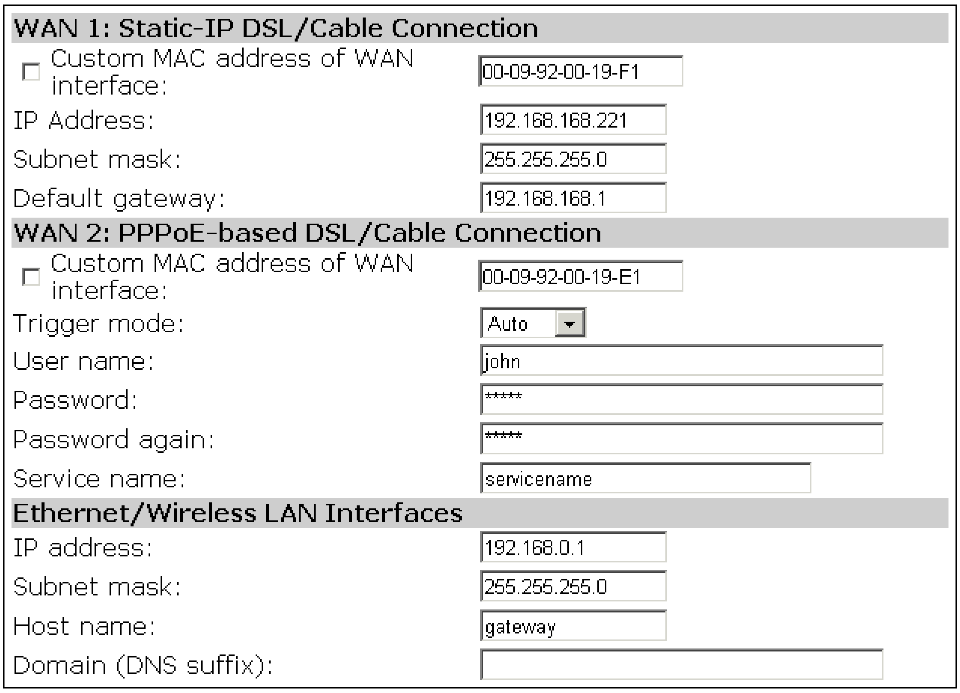
Fig. 50. TCP/IP settings for **Gateway with a Static-IP DSL/Cable Connection** mode.

If the gateway was set to be in **Gateway with a Static-IP DSL/Cable Connection** mode, two IP addresses are needed—one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it must be manually set. Consult your ISP for the correct **IP address**, **Default gateway**, **Subnet mask**, **Primary DNS server**, and **Secondary DNS server** settings.

Custom MAC Address of WAN Interface enables you to change the MAC address of the Ethernet WAN interface. Therefore, if the ISP-provided DSL or cable modem works only with the ISP-provided Ethernet card for a computer, the WAN interface of the gateway can mimic the ISP-provided Ethernet card by changing its MAC address to the Ethernet card's MAC address.

3.4.1.4. Gateway with Multiple DSL/Cable Connections



WAN 1: Static-IP DSL/Cable Connection	
□ Custom MAC address of WAN interface:	00-09-92-00-19-F1
IP Address:	192.168.168.221
Subnet mask:	255.255.255.0
Default gateway:	192.168.168.1
WAN 2: PPPoE-based DSL/Cable Connection	
□ Custom MAC address of WAN interface:	00-09-92-00-19-E1
Trigger mode:	Auto ▾
User name:	john
Password:	*****
Password again:	*****
Service name:	servicename
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.0.1
Subnet mask:	255.255.255.0
Host name:	gateway
Domain (DNS suffix):	

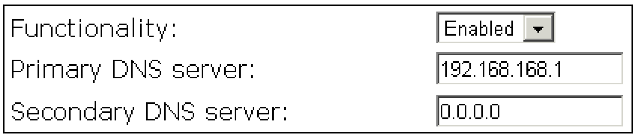
Fig. 51. TCP/IP settings for **Gateway with Multiple DSL/Cable Connections** mode.

Since the Internet connection can be PPPoE-based, DHCP-based, or Static-IP-based, the addressing settings of each WAN interface are the same as those of **Gateway with a PPPoE-Based DSL/Cable Connection**, **DHCP-Based DSL/Cable Connection**, or **Gateway with a Static-IP DSL/Cable Connection**, respectively. As a result, refer to Sections 3.4.1.1, 3.4.1.2, and 3.4.1.3 for more information.

3.4.2. DNS Proxy/Server

The DNS Proxy component of the gateway forwards DNS requests and reply messages between client computers and DNS servers. To client computers, the gateway acts like a DNS server. To DNS servers, the gateway acts like a client.

3.4.2.1. Basic



Functionality: Enabled

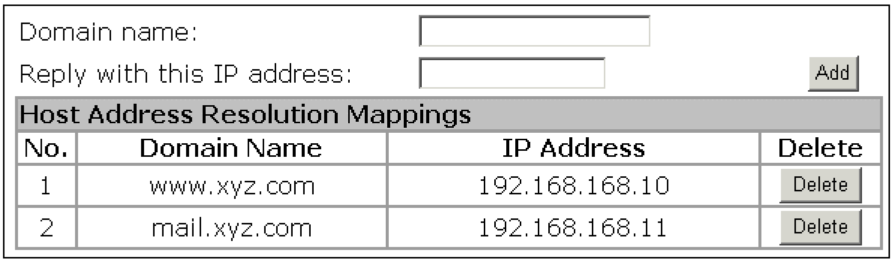
Primary DNS server: 192.168.168.1

Secondary DNS server: 0.0.0.0

Fig. 52. Basic DNS proxy settings.

In this section of the page, you specify the IP addresses of the DNS servers, when the gateway is in **Gateway with a Static-IP DSL/Cable Connection** mode. In other modes, the gateway obtains the DNS server information automatically from the ISP.

3.4.2.2. Host Address Resolution



Domain name:

Reply with this IP address:

Host Address Resolution Mappings

No.	Domain Name	IP Address	Delete
1	www.xyz.com	192.168.168.10	Delete
2	mail.xyz.com	192.168.168.11	Delete

Fig. 53. Host address resolution.

By **Host Address Resolution**, an internal server can be given a domain name, so that other hosts on the intranet can access the server by its domain name instead of by its IP address. For example, an internal Web server for the intranet, say 192.168.0.2, may be associated with the domain name, www.company-name.com.

To give an internal server a domain name:

1. Specify the domain name (**Domain name**) and the private IP address of the internal server (**Reply with this IP address**).

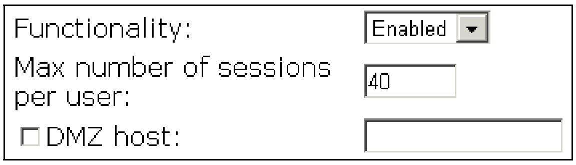
2. Click **Add** to add this entry to the **Host Address Resolution Mappings** table.

3. If you want to remove an entry from the table, click the corresponding **Delete** button.

NOTE: There is a hidden entry in the **Host Address Resolution Mappings** table, which maps "localhost.com" to the IP address of the LAN interface.

3.4.3. NAT Server

3.4.3.1. Basic



Functionality:	Enabled ▾
Max number of sessions per user:	40
□ DMZ host:	

Fig. 54. Basic NAT server settings.

When the gateway is in **Gateway with a Static-IP DSL/Cable Connection** mode, the NAT server functionality can be enabled or disabled.

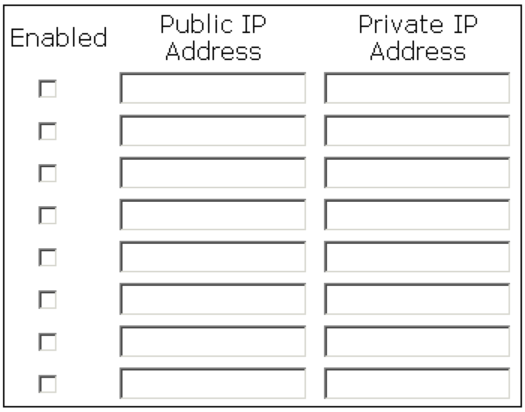
You can restrict the maximum number of user traffic sessions by specifying the **Max number of sessions per user** setting. In this way, you can prevent a single user from consuming too many network resources by initiating a large number of network sessions.

A DMZ (*DeMilitarized Zone*) host receives all unrecognized TCP/IP packets from the NAT server on the gateway; therefore TCP/IP networking applications running on the DMZ host would have better compatibility with NAT.

To specify the *DMZ host*:

- Enter the private IP address of the computer to be used as a DMZ host, and select the corresponding check box.

3.4.3.2. Static NAT Mappings



Enabled	Public IP Address	Private IP Address
□		
□		
□		
□		
□		
□		
□		
□		

Fig. 55. Static NAT mappings.

An ISP may provide more than one *public* IP address to its customer. A customer could use each of the public IP addresses for one type of server to be accessed from the Internet. This requirement can be satisfied by **Static NAT Mappings**. This functionality can be enabled only when the gateway is in **Gateway with a Static-IP DSL/Cable Connection** mode.

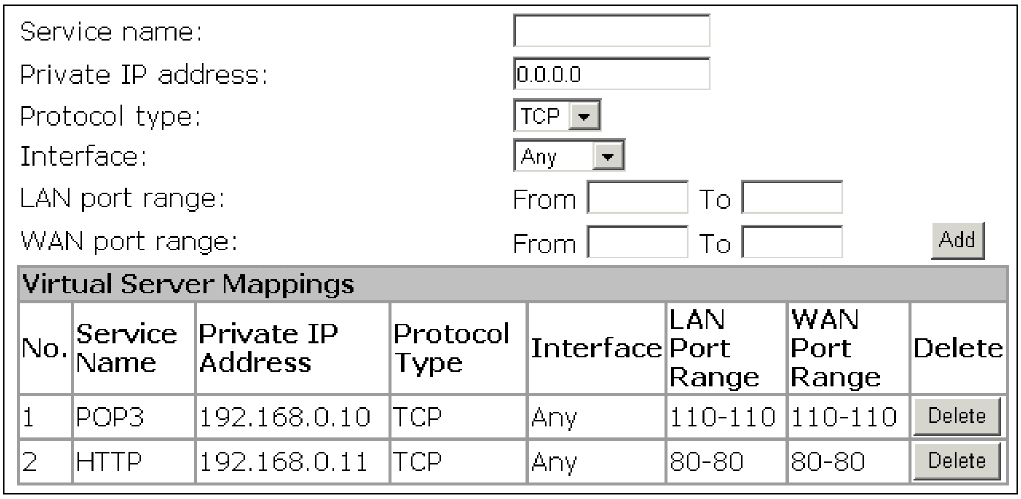
For example, say an ISP provides 5 public IP addresses, 61.16.33.114 to 61.16.33.118 inclusive, to its customer, ABC Technology. The network administrator of ABC Technology decides to use 61.16.33.114 for the multi-WAN wired broadband switch gateway, 61.16.33.115 for their public Web server, and 61.16.33.116 for their public POP3 server. And the administrator has registered with InterNIC (Internet Network Information Center) some domain name-to-IP address mappings—www.abc.com to 61.16.33.115 and pop3.abc.com to 61.16.33.116. However, the public Web server and POP3 server for ABC Technology sit on the intranet and use private IP addresses, 192.168.0.2 and 192.168.0.3, respectively. To expose the servers in this situation, the network administrator needs two static NAT mappings to associate 61.16.33.115 with 192.168.0.2 and 61.16.33.116 with 192.168.0.3.

To associate a public IP address with a private IP address:

1. Specify the public IP address and the private IP address for the association.

2. Select the corresponding **Enabled** check box.

3.4.3.3. Virtual Server Mappings



Service name:

Private IP address: 0.0.0.0

Protocol type: TCP

Interface: Any

LAN port range: From To

WAN port range: From To

Virtual Server Mappings

No.	Service Name	Private IP Address	Protocol Type	Interface	LAN Port Range	WAN Port Range	Delete
1	POP3	192.168.0.10	TCP	Any	110-110	110-110	Delete
2	HTTP	192.168.0.11	TCP	Any	80-80	80-80	Delete

Fig. 56. Virtual server mappings.

The gateway enables you to expose internal servers on the intranet through NAT to the Internet for public use. The exposed internal servers are called *virtual servers* because from perspective of hosts on the Internet, these servers are invisible in terms of TCP/IP. A server connection request from the Internet with a port within the specified *WAN port range* will be routed to the corresponding port within the specified *LAN port range* of the server on the intranet.

To expose an internal servers:

1. Give the service you want to expose a name in the **Service name** text box.

2. Specify the **Private IP address** of the internal servers.

3. Choose the **Protocol type** of the service.

4. Specify the WAN **Interface** that accepts this type of server connection requests.

5. Specify the **LAN port range** for the mapping by entering the **From** port and **End** port, inclusively.

6. Specify the **WAN port range** for the mapping by entering the **From** port and **End** port, inclusively.

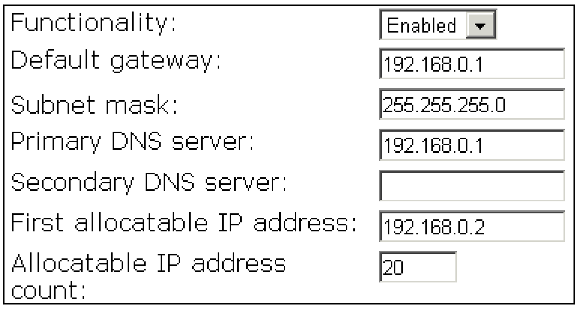
7. Click **Add**. And then you'll see the new mapping appears in the **Virtual Server Mappings** table.

To remove a virtual server mapping:

- Click **Delete** next to the mapping you want to remove.

3.4.4. DHCP Server

3.4.4.1. Basic



Functionality:	Enabled ▾
Default gateway:	192.168.0.1
Subnet mask:	255.255.255.0
Primary DNS server:	192.168.0.1
Secondary DNS server:	
First allocatable IP address:	192.168.0.2
Allocatable IP address count:	20

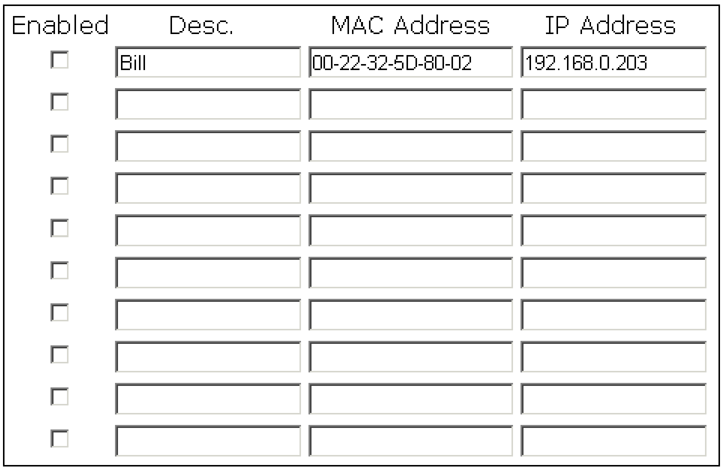
Fig. 57. Basic DHCP server settings.

The gateway can automatically assign IP addresses to client computers by DHCP. In this section of the management page, you can specify the **Default gateway**, **Subnet mask**, **Primary DNS server**, and **Secondary DNS server** settings that will be sent to a client at its request. Additionally, you can specify the first IP address that will be assigned to the clients and the number of allocateable IP addresses.

In most cases, **Default gateway** and **Primary DNS server** should be set to the IP address of the gateway's LAN interface (e.g., the default LAN IP address is **192.168.0.1**), and **Subnet mask** is set to **255.255.255.0**.

NOTE: There should be only *one* DHCP server on the LAN; otherwise, DHCP would not work properly. If there is already a DHCP server on the LAN, disable the DHCP server functionality of the gateway.

3.4.4.2. Static DHCP Mappings



Enabled	Desc.	MAC Address	IP Address
□	Bill	00-22-32-5D-80-02	192.168.0.203
□			
□			
□			
□			
□			
□			
□			
□			
□			

Fig. 58. Static DHCP mappings.

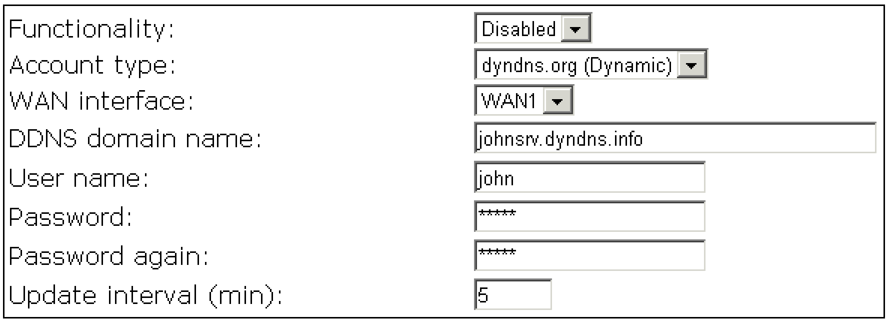
IP addresses of servers are often static so that clients could always locate the servers by the static IP addresses. By **Static DHCP Mappings**, you can ensure that a host will get the same IP address when it requests one from the DHCP server. Therefore, instead of configuring the IP address of an intranet server manually, you can configure the server to obtain an IP address by DHCP and it is always assigned the same IP address.

To always assign a static IP address to a specific DHCP client:

1. Specify the MAC address of the DHCP client and the IP address to be assigned to it. Then, give a description for this mapping.

2. Select the corresponding **Enabled** check box.

3.4.5. Dynamic DNS



Functionality:	Disabled
Account type:	dyndns.org (Dynamic)
WAN interface:	WAN1
DDNS domain name:	johnsrv.dyndns.info
User name:	john
Password:	*****
Password again:	*****
Update interval (min):	5

Fig. 59. Dynamic DNS settings.

With the help of dynamic DNS (DDNS) services provided by *dyndns.org* or *no-ip.com*, you can make your device automatically register the IP address it obtains dynamically by PPPoE or DHCP with the DDNS servers. DDNS is useful if you want to set up a Web server whose IP address is dynamically obtained rather than statically configured.

Choose your DDNS service provider from the **Account type** drop-down list, choose the **WAN interface** on which the DDNS client operates, and specify the **DDNS domain name**, **User name**, and **Password** you have registered with your service provider. The DDNS client of the gateway periodically communicates with its DDNS server at an interval specified by the **Update interval** setting.

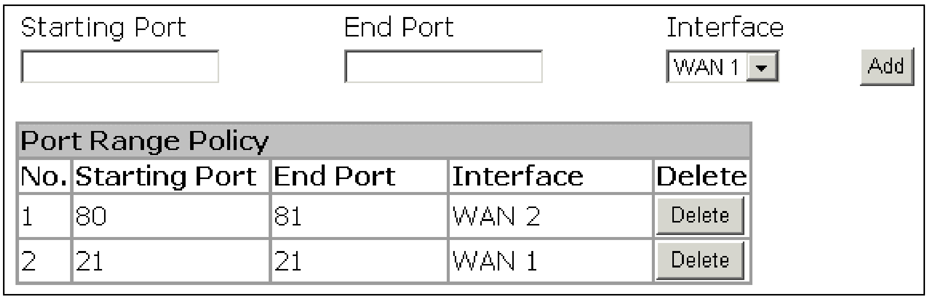
3.4.6. Bandwidth Management

3.4.6.1. LAN-to-WAN Load Balancing

You can specify policies for forcing specific LAN-to-WAN traffic to go out to the Internet through a specific WAN interface when the gateway is configured to be in a multi-WAN mode. LAN-to-WAN traffic can be classified *by port range* or *by IP address range*.

NOTE: A by-port-range policy has priority over a by-IP-address-range policy from the perspective of the load-balancing engine.

Policy by Port Range



Port Range Policy

No.	Starting Port	End Port	Interface	Delete
1	80	81	WAN 2	Delete
2	21	21	WAN 1	Delete

Fig. 60. By-port-range policy settings for LAN-to-WAN load balancing.

To specify a by-port-range policy:

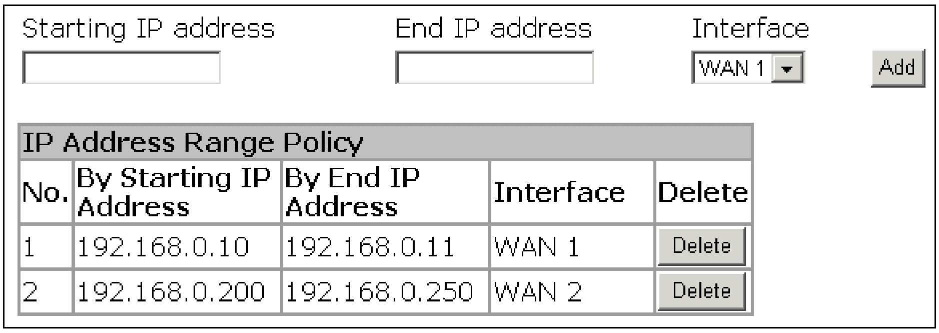
1. Specify the **Starting Port**, **End Port**, and the WAN **Interface** for this kind of LAN-to-WAN traffic.

2. Click **Add**.

3. Then this policy will be shown in the **Port Range Policy** table.

4. If you want to remove this policy, click the corresponding **Delete** button.

Policy by IP Address Range



IP Address Range Policy

No.	By Starting IP Address	By End IP Address	Interface	Delete
1	192.168.0.10	192.168.0.11	WAN 1	Delete
2	192.168.0.200	192.168.0.250	WAN 2	Delete

Fig. 61. By-IP-address-range policy settings for LAN-to-WAN load balancing.

To specify a by-IP-address-range policy:

1. Specify the **Starting IP address**, **End IP address**, and the WAN **Interface** for this kind of LAN-to-WAN traffic.

2. Click **Add**.

3. Then this policy will be shown in the **Port Range Policy** table.

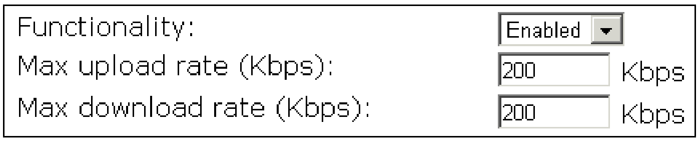
4. If you want to remove this policy, click the corresponding **Delete** button.

3.4.6.2. Client Bandwidth Control

By *Client Bandwidth Control*, you can limit the network bandwidth each client can consume in Kbps (Kilo-bit per second). This function can prevent a single user from occupying all network bandwidth. The bandwidth control policy can be *all-users-wide* or *on a per user basis*.

To specify a bandwidth control policy, you specify a **Max upload rate** and a **Max download rate** for upstream and downstream traffic, respectively.

Basic



Functionality: Enabled

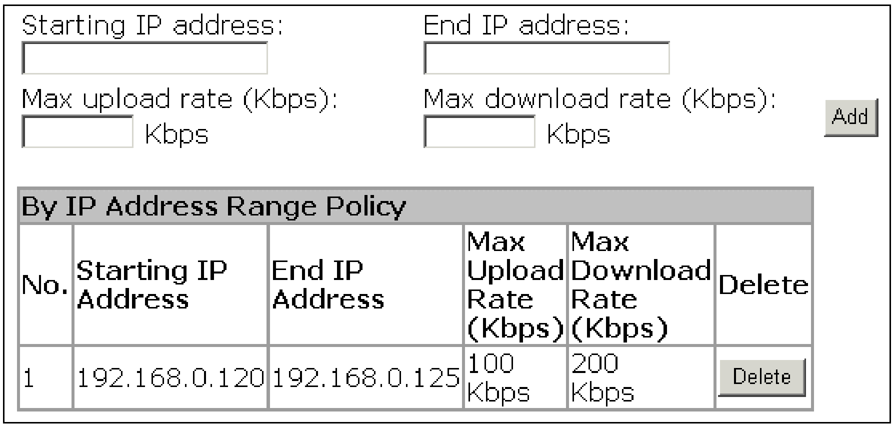
Max upload rate (Kbps): 200 Kbps

Max download rate (Kbps): 200 Kbps

Fig. 62. Basic client bandwidth control settings.

The *basic* bandwidth control policy is applied to all users except for those are controlled by the *by-IP-address-range* policy and the *by-MAC-address* policy.

Policy by IP Address Range



Starting IP address:

End IP address:

Max upload rate (Kbps): Kbps

Max download rate (Kbps): Kbps

By IP Address Range Policy

No.	Starting IP Address	End IP Address	Max Upload Rate (Kbps)	Max Download Rate (Kbps)	Delete
1	192.168.0.120	192.168.0.125	100 Kbps	200 Kbps	Delete

Fig. 63. By-IP-address-range policy settings for client bandwidth control.

To specify a by-IP-address-range policy:

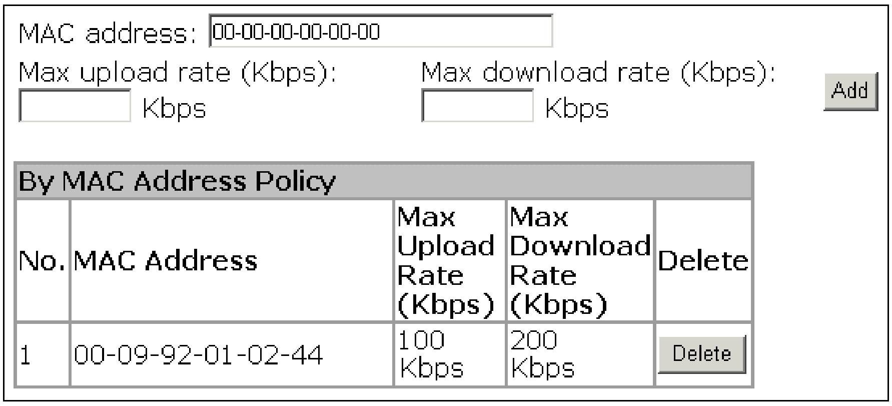
1. Specify the **Starting IP address**, **End IP address**, **Max upload rate** and **Max download rate** for the clients to limit their maximum bandwidth consumption.

2. Click **Add**.

3. Then this policy will be shown in the **By IP Address Range Policy** table.

4. If you want to remove this policy, click the corresponding **Delete** button.

Policy by MAC Address



MAC address: 00-00-00-00-00-00

Max upload rate (Kbps): Kbps

Max download rate (Kbps): Kbps

By MAC Address Policy

No.	MAC Address	Max Upload Rate (Kbps)	Max Download Rate (Kbps)	Delete
1	00-09-92-01-02-44	100 Kbps	200 Kbps	Delete

Fig. 64. By-MAC-address policy for client bandwidth control.

To specify a by-MAC-address policy:

5. Specify the **MAC address**, **Max upload rate**, and **Max download rate** for the client to limit its maximum bandwidth consumption.

6. Click **Add**.

7. Then this policy will be shown in the **By MAC Address Policy** table.

8. If you want to remove this policy, click the corresponding **Delete** button.

3.4.7. PPTP Client

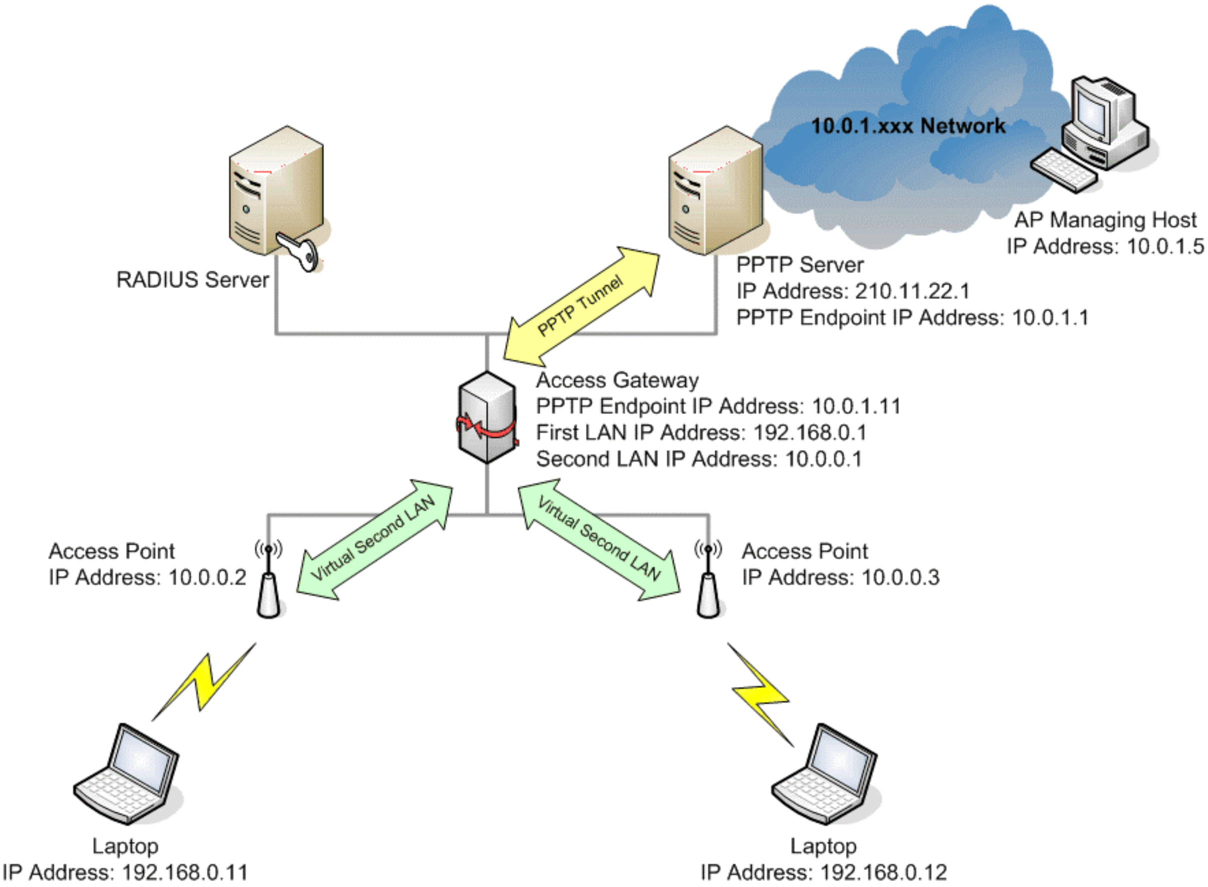


Fig. 65. PPTP and Virtual Second LAN.

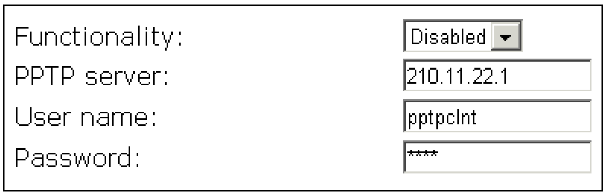
By PPTP and Virtual Second LAN, a WISP can securely manage access points behind the access gateway that acts as an NAT server.

As illustrated in Fig. 65, the access gateway exposes two LAN-side private networks—one is for the wireless clients (*Physical First LAN*: 192.168.0.xxx) and the other is for the access points (*Virtual Second LAN*: 10.0.0.xxx). The two private networks are separated so that now traffic is allowed between the two private networks. This way, a hacker on the 192.168.0.xxx network cannot attack access points on the 10.0.0.xxx network.

After the PPTP client of the access gateway establishes a PPTP tunnel with a remote PPTP server (i.e., 210.22.11.1), a *static route* between the PPTP tunnel (10.0.1.11) and the virtual second LAN (10.0.0.1) is created. Thereafter, any host (ex., 10.0.1.5) on the remote 10.0.1.xxx network can reach the access points on the 10.0.0.xxx network for access point management purposes. And all management packets are encrypted when transmitted in the PPTP tunnel.

TIP: Alternatively, you can use an NAT port mapping-based way for behind-NAT access point management. See Section 3.7.4 for more information.

3.4.7.1. Basic



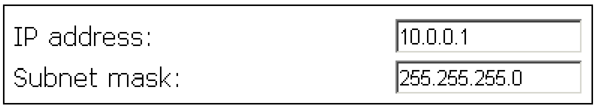
Functionality:	Disabled
PPTP server:	210.11.22.1
User name:	pptpclnt
Password:	****

Fig. 66. Basic PPTP client settings.

To establish a PPTP tunnel with a remote PPTP server, specify the IP address of the **PPTP server**, **user name** and **password** for authentication. And then, enable the PPTP client **Functionality**.

NOTE: Configure your PPTP server to use MS-CHAPv1 as the authentication method and to assign IP addresses to PPTP clients.

3.4.7.2. Virtual Second LAN

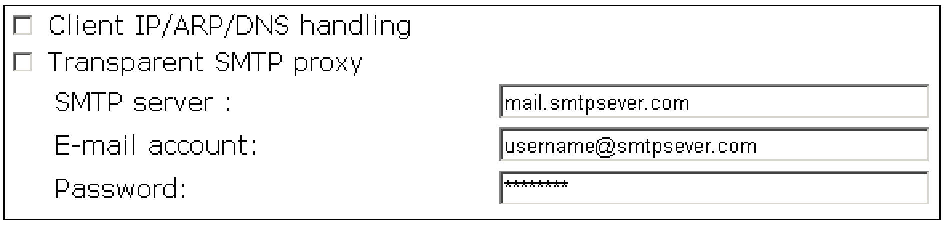


IP address:	10.0.0.1
Subnet mask:	255.255.255.0

Fig. 67. Virtual second LAN settings.

Specify the **IP address** and **Subnet mask** of the virtual second LAN interface to enable the virtual second LAN.

3.4.8. Zero Client Reconfiguration



□ Client IP/ARP/DNS handling

□ Transparent SMTP proxy

SMTP server :	mail.smtpsever.com
E-mail account:	username@smtpsever.com
Password:	********

Fig. 68. Zero client reconfiguration settings.

When *Zero Client Reconfiguration* function is enabled, the gateway ignores IP, DNS (**Client IP/ARP/DNS handling**), and/or SMTP (Simple Mail Transfer Protocol) (**Transparent SMTP proxy**) settings of client computers. As a result, the configuration of a client computer need not be changed to access the Internet through the gateway.

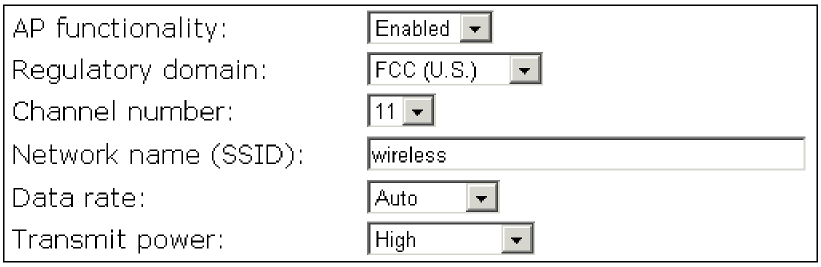
When **Transparent SMTP proxy** is enabled, you have to specify the SMTP server (identified by domain name or IP address) to which SMTP traffic from clients will be redirected. If the SMTP needs authentication, you have to specify the **E-mail account** and **password** as well.

3.5. Configuring IEEE 802.11b-Related Settings

3.5.1. Communication

3.5.1.1. Basic

IEEE 802.11b-related communication settings include **AP functionality**, **Regulatory domain**, **Channel number**, and **Network name (SSID)**, **Data rate**, and **Transmit power**.



AP functionality:	Enabled
Regulatory domain:	FCC (U.S.)
Channel number:	11
Network name (SSID):	wireless
Data rate:	Auto
Transmit power:	High

Fig. 69. IEEE 802.11b communication settings.

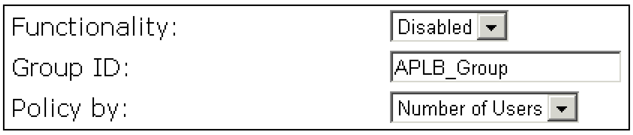
For specific needs such as configuring the wireless access gateway as a wireless LAN-to-LAN bridge, the AP functionality can be disabled, so that no wireless client can associate with the wireless access gateway.

The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. The SSID of a wireless client computer and the SSID of the wireless access gateway must be identical for them to communicate with each other.

The maximum data rate of IEEE 802.11b is 11Mbps. In case there is RF interference, you may want to reduce the data rate to 5.5Mbps, 2Mbps, or 1Mbps. We suggest this setting be configured to **Auto** for better performance in most situations.

The transmit power of the RF module of the wireless access gateway can be adjusted so that the RF coverage of the gateway can be changed.

3.5.1.2. AP Load Balancing



Functionality:	Disabled
Group ID:	APLB_Group
Policy by:	Number of Users

Fig. 70. AP load balancing settings.

Several wireless access gateways and APs can form a load-balancing group if they are set the same **Group ID**. The load-balancing policy can be by *Number of Users* or by *Traffic Load.*

If the *by-number-of-users* policy is selected, a new wireless user can only associate with an AP that has the smallest number of associated wireless users in the group. On the other hand, if the *by-traffic-load policy* is selected, a new wireless user can only associate with an AP that has the less traffic load in the group.

3.5.1.3. Wireless Distribution System

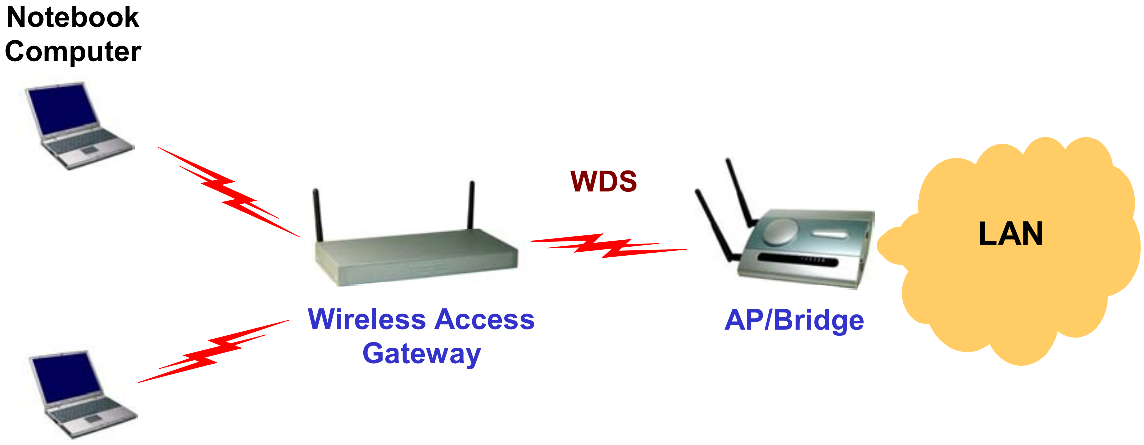
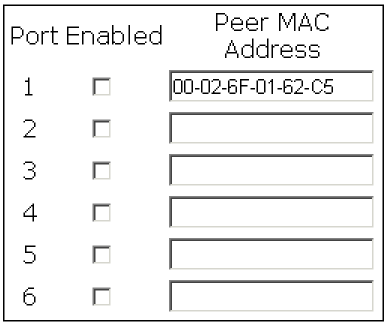


Fig. 71. Wireless Distribution System.

Traditionally, access points are connected by Ethernet. By Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, in Fig. 71, the wireless access gateway acts as an access point for the notebook computers and it forwards packets sent from the notebook computers to the AP/bridge through WDS. Then, the AP/bridge forwards the packets to the Ethernet LAN. Packets destined for the notebook computers follow a reverse path from the Ethernet LAN through the wireless access gateway to the notebook computers. In this way, the wireless access gateway plays a role of "AP repeater."

NOTE: The wireless access gateway can have up to *6* WDS links to other wireless AP/bridge.



Port	Enabled	Peer MAC Address
1	□	00-02-6F-01-62-C5
2	□	
3	□	
4	□	
5	□	
6	□	

Fig. 72. Wireless Distribution System settings.

To enable a WDS link:

1. Specify the MAC address of the AP or wireless bridge at the other end of the WDS link.

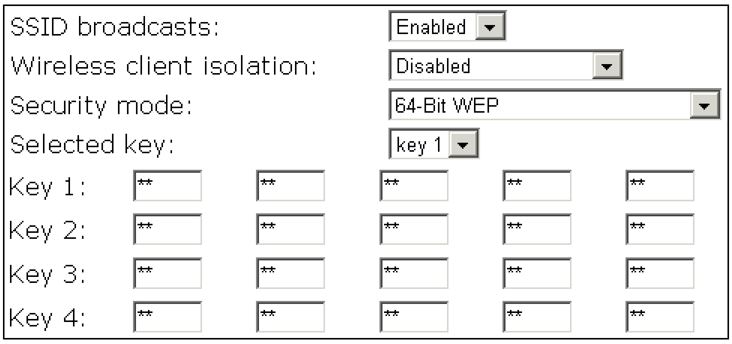
2. Select the corresponding **Enabled** check box.

For example, assume you want a wireless access gateway and an AP with MAC addresses 00-02-65-01-62-C5 and 00-02-65-01-62-C6, respectively, to establish a WDS link between them. On Gateway 00-02-65-01-62-C5, set the peer MAC address of port 1 to 00-02-65-01-62-C6 and on AP 00-02-65-01-62-C6, set the peer MAC address of port 1 to 00-02-65-01-C5.

TIP: Plan your wireless network and draw a diagram, so that you know how a wireless access gateway is connected to other peer APs or wireless bridges by WDS.

3.5.2. Security

3.5.2.1. Basic



SSID broadcasts:	Enabled				
Wireless client isolation:	Disabled				
Security mode:	64-Bit WEP				
Selected key:	key 1				
Key 1:	**	**	**	**	**
Key 2:	**	**	**	**	**
Key 3:	**	**	**	**	**
Key 4:	**	**	**	**	**

Fig. 73. IEEE 802.11b basic security settings.

For security reasons, it's highly recommended that the security mode be set to options other than *Open System*. When the security mode is set to Open System, no authentication and data encryption will be performed. Additionally, you can *disable* the SSID broadcasts functionality so that a wireless client computer with an "any" SSID cannot associate with the wireless access gateway.

When the **Wireless client isolation** setting is set to *This AP only*, wireless clients of this wireless access gateway as an AP cannot see each other, and wireless-to-wireless traffic is blocked. When the setting is set to *All APs in this subnet*, traffic among wireless users of different APs in the same IP subnet is blocked. This feature is useful for WLANs deployed in public places. In this way, hackers have no chance to attack other wireless users in a *hotspot*. The behaviors are illustrated in the following figures.

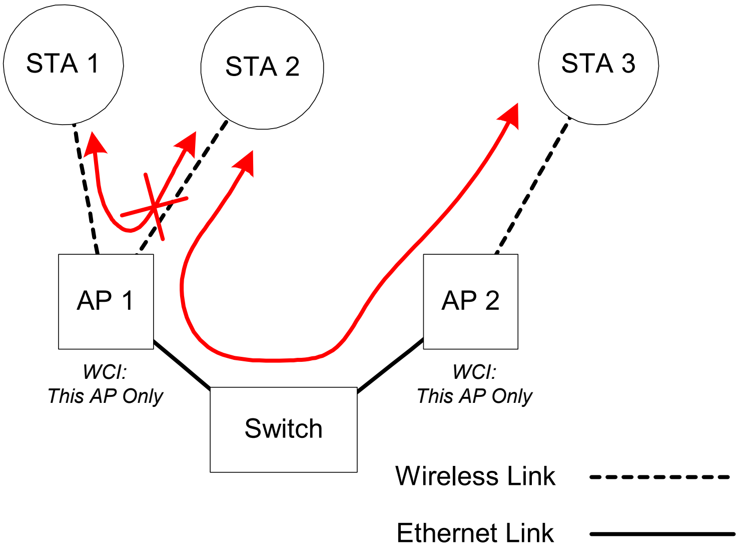


Fig. 74. Behavior of the "This AP Only" wireless client isolation option.

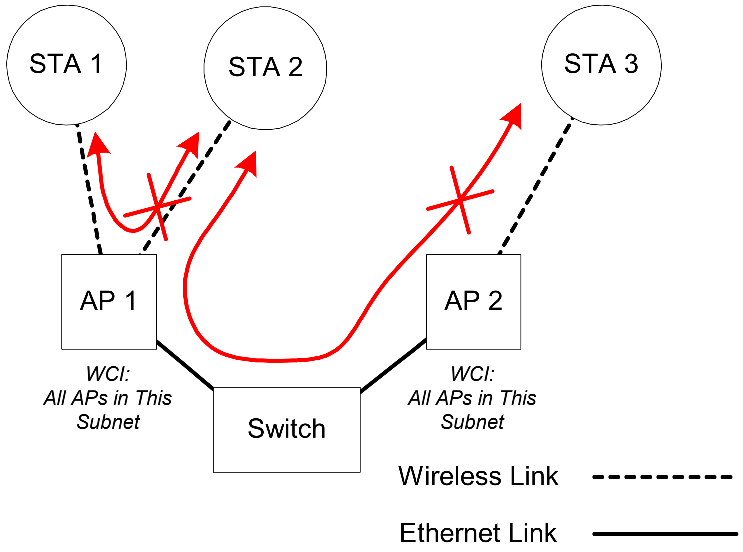


Fig. 75. Behavior of the “All APs on This Subnet” wireless client isolation option.

As illustrated in Fig. 74 when AP 1 and AP 2 are using the “This AP Only” option, wireless traffic between STA 1 and STA 2 is blocked by AP 1, while wireless traffic between STA 2 and STA 3, which are associated with different APs, is still allowed. If the “All APs in This Subnet” option is used as shown in Fig. 75, AP 1 and AP 2 communicates with each other via an inter-AP protocol to share their STA association information to block wireless traffic among all the STAs.

There are up to 9 security modes depending on wireless access gateway model variations:

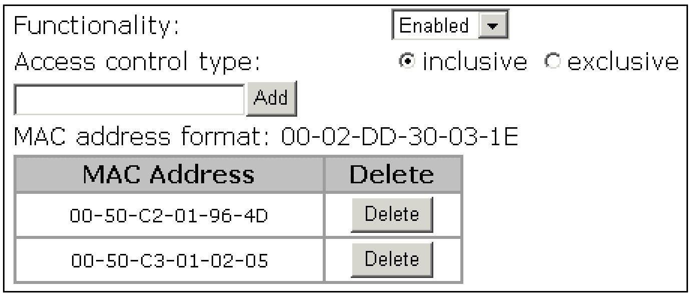
- **Open System.** No authentication, no data encryption.
- **64-bit WEP.** Authentication and data encryption based on 64-bit WEP (Wired Equivalent Privacy).
- **128-bit WEP.** Authentication and data encryption based on 128-bit WEP (Wired Equivalent Privacy), and 128-bit keys are used.
- **802.1x EAP-MD5.** The IEEE 802.1x functionality is enabled and the username/password-based EAP-MD5 authentication is used. No data encryption.
- **802.1x EAP-MD5 + 64-Bit WEP.** The IEEE 802.1x functionality is enabled and the username/password-based EAP-MD5 authentication is used. Data encryption is achieved by 64-bit WEP.
- **802.1x EAP-MD5 + 128-Bit WEP.** The IEEE 802.1x functionality is enabled and the username/password-based EAP-MD5 authentication is used. Data encryption is achieved by 128-bit WEP.
- **802.1x EAP-TLS; No Encryption.** The IEEE 802.1x functionality is enabled and the digital certificate-based EAP-TLS user authentication. No data encryption is used.
- **802.1x EAP-TLS 64-Bit Key.** The IEEE 802.1x functionality is enabled and the digital certificate-based EAP-TLS (Transport Layer Security) user authentication and data encryption is used. Session keys are 64-bit.
- **802.1x EAP-TLS 128-Bit Key.** The IEEE 802.1x functionality is enabled and the digital cer-

tificate-based EAP-TLS user authentication and data encryption is used. Session keys are 128-bit.

See Section 3.5.2.3 for more information about IEEE 802.1x.

NOTE: Each field of a WEP key setting is a *hex-decimal* number from 00 to FF. For example, when the security mode is set to **64-bit WEP**, you could set Key 1 to "00 01 2E 3A DF".

3.5.2.2. MAC-Address-Based Access Control



Functionality: Enabled

Access control type: ● inclusive ○ exclusive

MAC address format: 00-02-DD-30-03-1E

MAC Address	Delete
00-50-C2-01-96-4D	Delete
00-50-C3-01-02-05	Delete

Fig. 76. MAC-address-based access control settings.

With **MAC-Address-Based Access Control**, you can specify the wireless client computers that are permitted or not permitted to associate with the wireless access gateway. When the table type is set to *inclusive*, entries in the table are permitted to associate with the wireless access gateway. When the table type is set to *exclusive*, entries in the table are not permitted to associate with the wireless access gateway.

To *deny* wireless clients' access to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.

2. Set the **Access control type** to *exclusive*.

3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.

4. Repeat Steps 3 for other wireless clients.

To *grant* wireless clients' access to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.

2. Set the **Access control type** to *inclusive*.

3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.

4. Repeat Steps 3 for other wireless clients.

To delete an entry in access control table:

- Click **Delete** next to the entry.

3.5.2.3. IEEE 802.1x

IEEE 802.1x *Port-Based Network Access Control* is a new standard for solving some security issues associated with IEEE 802.11, such as lack of user-based authentication and dynamic encryption key distribution. With IEEE 802.1x and the help of a RADIUS (Remote Authentication Dial-In User Service) server and a user account database, an enterprise or ISP (Internet Service Provider) can manage its mobile users' access to its wireless LANs. Before granted access to a wireless LAN supporting IEEE 802.1x, a user has to issue his or her *user name* and *password* or *digital certificate* to the backend RADIUS server by EAPOL (Extensible Authentication Protocol Over LAN). The RADIUS server can record accounting information such as when a user logs on to the wireless LAN and logs off from the wireless LAN for monitoring or billing purposes.

The IEEE 802.1x functionality of the wireless access gateway is controlled by the *security mode* (see Section 3.5.2.1). So far, the wireless access gateway supports two authentication mechanisms—EAP-MD5 (Message Digest version 5) and EAP-TLS (Transport Layer Security) for IEEE 802.1x. If EAP-MD5 is used, the user has to give his or her *user name* and *password* for authentication. If EAP-TLS is used, the wireless client computer automatically gives the user's *digital certificate* that is stored in the computer hard disk or a smart card for authentication. And after a successful EAP-TLS authentication, a session key is automatically generated for wireless packets encryption between the wireless client computer and its associated wireless access gateway. To sum up, EAP-MD5 supports only user authentication, while EAP-TLS supports user authentication as well as dynamic encryption key distribution.

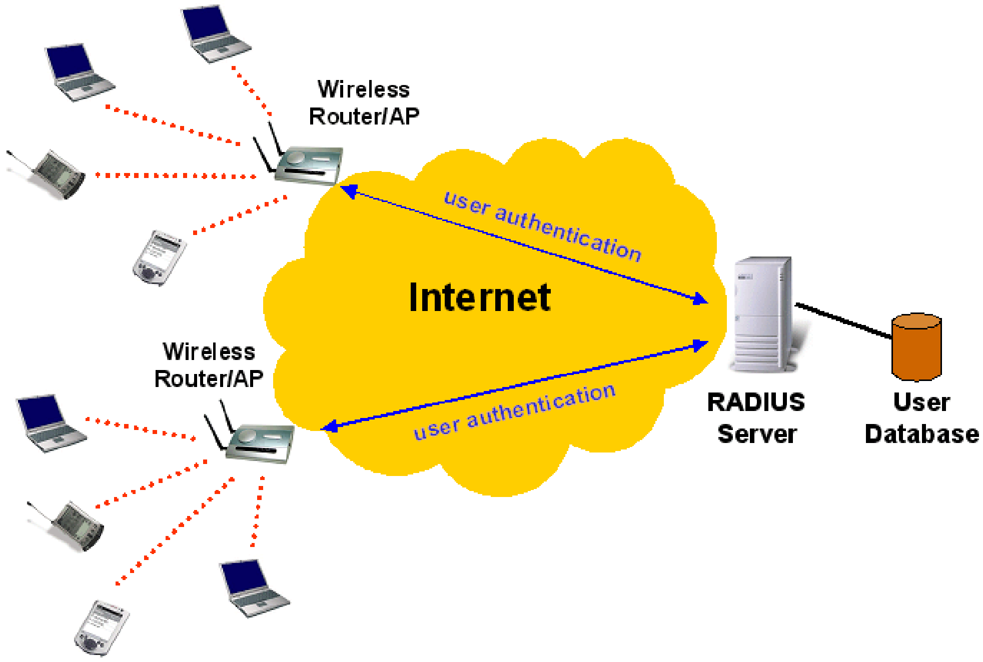


Fig. 77. IEEE 802.1x and RADIUS.

TIP: Go to the **Authentication, RADIUS** section of the Web management UI to configure RADIUS settings (see Section 3.6.2).

TIP: Refer to the IEEE 802.1x-related white papers on the accompanying CD-ROM for more information about deploying secure WLANs with IEEE 802.1x support.

3.6. Configuring Authentication Settings

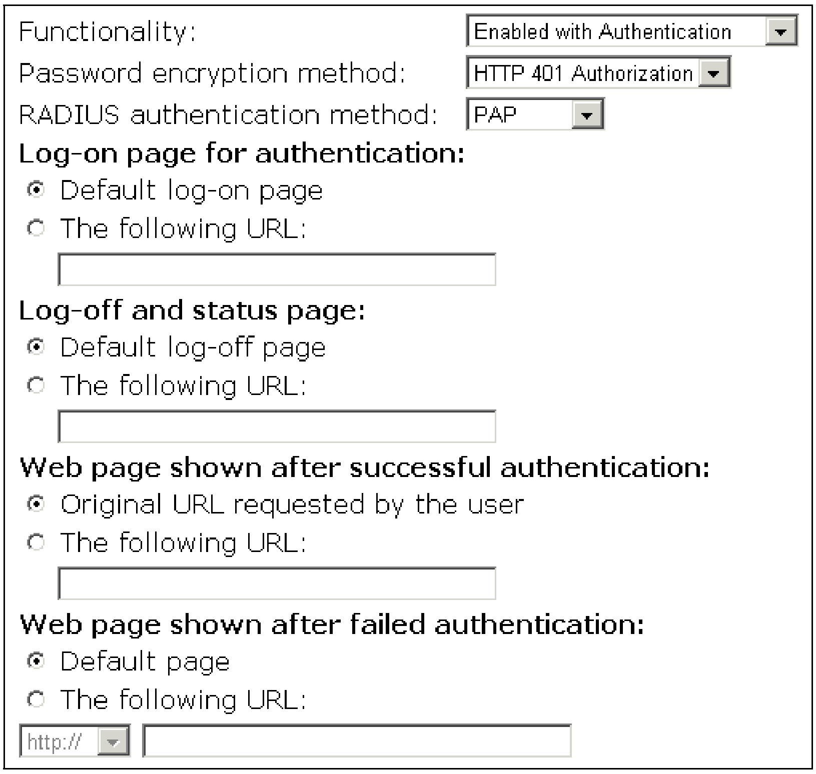
All models of the access gateway support Web redirection-based user authentication. Furthermore, the *advanced* edition of the wireless access gateway, which has a built-in access point, supports IEEE 802.1x-based user authentication.

Here is a brief description of how Web redirection works: When an unauthenticated wireless user is trying to access a Web page, a logon page is shown instead of the requested page, so that the user can type his/her user name and password for authentication. Then, the user credential information is sent to a back-end RADIUS (Remote Authentication User Dial-In Service) server to see if the wireless user is allowed to access the Internet. The authentication mechanism employed for RADIUS is EAP-MD5, PAP, or CHAP.

TIP: For IEEE 802.1x-based user authentication, see Section 3.5.2.3.

3.6.1. Web Redirection

3.6.1.1. Basic



Functionality: Enabled with Authentication

Password encryption method: HTTP 401 Authorization

RADIUS authentication method: PAP

Log-on page for authentication:

● Default log-on page

○ The following URL:

Log-off and status page:

● Default log-off page

○ The following URL:

Web page shown after successful authentication:

● Original URL requested by the user

○ The following URL:

Web page shown after failed authentication:

● Default page

○ The following URL:

http://

Fig. 78. Web redirection enabled with authentication.

There are three modes for Web redirection—**Enabled with Authentication**, **Enabled without Authentication**, and **Disabled**.

In **Enabled with Authentication** mode, you specify the **RADIUS authentication method** that corresponds to your RADIUS server settings. Currently EAP-MD5, PAP, and CHAP are supported. And you can choose the way username and password information from clients is encrypted:

- **HTTP 401 Authorization.** In this mode, the 401 authorization method specified in the HTTP standard is used for challenging the user his/her username and password. The username and password information is encrypted by the Base64 algorithm. After the **Log On** button on the log-on page is clicked, a window appears for the user to enter his/her username and password.

- **CGI without Encryption.** In this mode, the user enters his/her username and password directly on the log-on page, and then clicks the **Log On** button to log on. The username and password information is transmitted from the client computer to the gateway in plaintext.

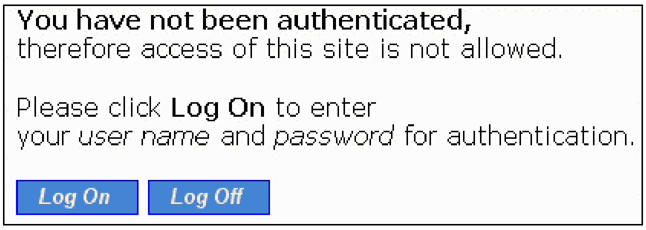
- **CGI with Base64.** In this mode, the user enters his/her username and password directly on the log-on page, and then clicks the **Log On** button to log on. The username and password information transmitted from the client computer to the gateway is encrypted by the Base64 algorithm.

- **CGI with SSL.** In this mode, the user enters his/her username and password directly on the log-on page, and then clicks the **Log On** button to log on. The username and password information transmitted from the client computer to the gateway is encrypted by SSL (Secure Socket Layer).

NOTE: The gateway is equipped with a default certificate and a private key for SSL operations. As an alternative, you can use a certificate file and a private key file, both of which issued by a CA (Certificate Authority) that you trust. Section 3.3.3.6 describes how to upload a certificate file and a private key file to the gateway.

TIP: If you have uploaded a certificate file and a private file to the gateway and the **CGI with SSL** option is chosen, make sure the *host name* and *domain (DNS suffix)* settings of the gateway's LAN interface correspond with those contained in the certificate file. This way, the Web browser on the client computer will not warn the user to verify the certificate during SSL handshaking between the gateway and the client computer.

When a wireless user tries to access the Internet, he/she is redirected to a **Default log-on page** or a page stored on an external Web server (**The following URL**), depending on the network administrator's choice.


You have not been authenticated,
therefore access of this site is not allowed.

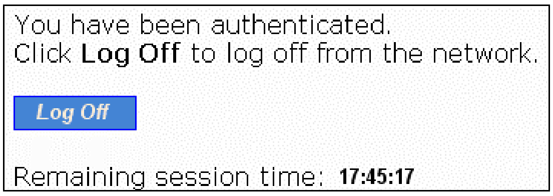
Please click **Log On** to enter
your *user name* and *password* for authentication.

Fig. 79. Default log-on page.

NOTE: If the **CGI with SSL** mode is chosen and an external log-on page is used, make sure the URL of the external log-on page is HTTPS-based.

After the wireless user passes authentication, the wireless user can be brought to the originally requested Web page (**Original URL requested by the user**) or to a default page for advertisement purposes (**The following URL**). For example, if "http://www.wi-fi.com" is set for **The following URL**, the user will be brought to the home page of Wi-Fi Alliance.

In addition, the **Log-Off** window is also shown after the wireless passes authentication. The **Log-Off** window can be configured to contain the **Default log-off page** or a page stored on an external Web server (**The following URL**).



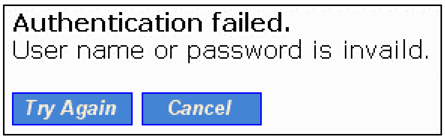
You have been authenticated.
Click **Log Off** to log off from the network.

Remaining session time: **17:45:17**

Fig. 80. Default log-off page.

NOTE: On a PDA such as Pocket PC, the log-off would not be shown. To log off from the network, go back to the log-on page, and then click **Log Off** to end the session.

If the user fails the authentication, the user can be brought to a default warning page (**Default page**) or a page for the user to subscribe a wireless Internet access service (**The following URL**).

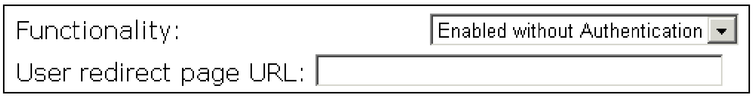


Authentication failed.
User name or password is invaild.

Fig. 81. Default authentication failure warning page.

NOTE: If you choose **The following URL** for **Log-on page for authentication**, **Log-off and status page**, or **Web page shown after failed authentication**, the pages stored on an external server have to contain specific HTML/JavaScript code so that Web redirection can work without error. Use the source of the default pages as templates for design your own authentication pages.

NOTE: Because your customized versions of authentication pages have to contain references to the access gateway's LAN IP address (**192.168.0.1** by default). If the LAN IP address of the access gateway is changed, you must remember to change the IP address references in you customized pages.

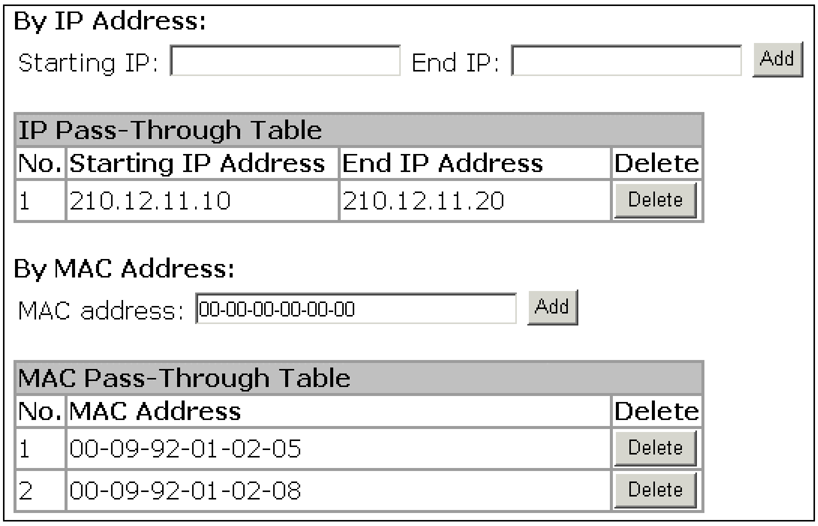


Functionality: Enabled without Authentication
User redirect page URL:

Fig. 82. Web redirection enabled without authentication.

In **Enabled without Authentication** mode, a user can access the Internet through the access gateway without being authenticated first. However, instead of accessing his/her requested page, he/she is first redirected to a URL for advertisement purposes (**User redirect page URL**).

3.6.1.2. Unrestricted Clients



By IP Address:

Starting IP: End IP:

IP Pass-Through Table			
No.	Starting IP Address	End IP Address	Delete
1	210.12.11.10	210.12.11.20	Delete

By MAC Address:

MAC address: 00-00-00-00-00-00

MAC Pass-Through Table		
No.	MAC Address	Delete
1	00-09-92-01-02-05	Delete
2	00-09-92-01-02-08	Delete

Fig. 83. Unrestricted clients settings.

There are occasions on which you want some computers to be able to freely access the Internet without being authenticated first. For example, you may want your wired desktop computers connected with the gateway to be uncontrolled by the gateway while providing wireless Internet access service for your customers with wireless laptop computers. The **Unrestricted Clients** feature is for this purpose.

You can specify the computers to be uncontrolled by IP address or MAC address.

To specify uncontrolled computers within an IP address range:

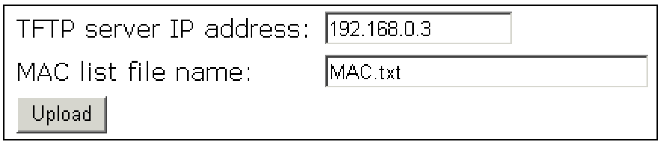
1. Specify the **Stating IP** and **End IP** addresses of the IP address range.

2. Click **Add**. Then you'll see the newly entered IP address range appear in the **IP Pass-Though Table**.

To specify a uncontrolled computer by MAC address:

1. Specify its **MAC address**.

2. Click **Add**. Then you'll see the newly entered MAC address appear in the **MAC Pass-Through Table**.

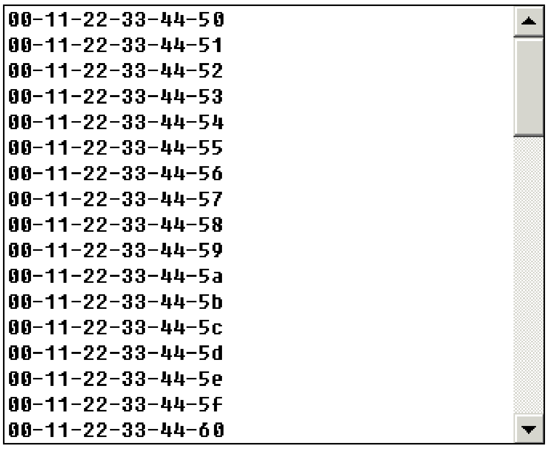


TFTP server IP address: 192.168.0.3

MAC list file name: MAC.txt

Fig. 84. MAC address list upload settings.

Instead of manually entering MAC addresses to the MAC pass-through table one by one, you can prepare a text file that contains all the MAC addresses and put it on a TFTP server, and then upload the MAC address list file from the TFTP server to the access gateway. Fig. 85 shows the contents of a sample MAC address list file.



```
00-11-22-33-44-50
00-11-22-33-44-51
00-11-22-33-44-52
00-11-22-33-44-53
00-11-22-33-44-54
00-11-22-33-44-55
00-11-22-33-44-56
00-11-22-33-44-57
00-11-22-33-44-58
00-11-22-33-44-59
00-11-22-33-44-5a
00-11-22-33-44-5b
00-11-22-33-44-5c
00-11-22-33-44-5d
00-11-22-33-44-5e
00-11-22-33-44-5f
00-11-22-33-44-60
```

Fig. 85. Sample MAC address list file.

To upload a MAC address list file from a TFTP server:

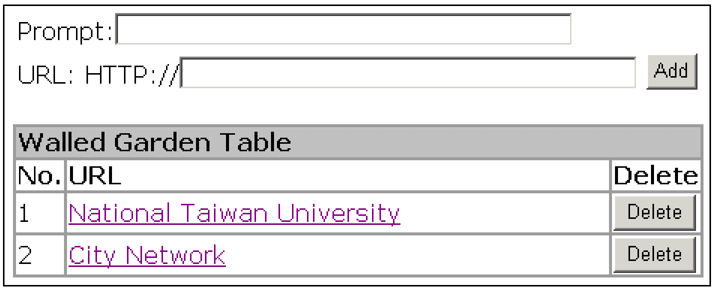
1. Specify the IP address of the TFTP server in the **TFTP server IP address** text box.

2. Specify the name of the MAC ACL file on the TFTP server in the **MAC list file name** text box.

3. Click **Upload**.

NOTE: The **MAC Pass-Through Table** can contain up to 100 MAC address entries.

3.6.1.3. Walled Garden



Prompt:

URL: HTTP://

Walled Garden Table		
No.	URL	Delete
1	National Taiwan University	Delete
2	City Network	Delete

Fig. 86. Walled garden settings.

IP addresses or URLs in the *walled garden* can be accessed without authentication. This feature is useful for WISPs to do advertisement. For example, a WISP can set up a Web server to contain advertisement information for users who have not subscribed to its wireless Internet access service. The walled garden links are shown on the *log-on* authentication page.

To add a link to the walled garden:

1. Describe this link in the **Prompt** text box.

2. Specify the URL of this link in the **URL** text box.

3. Click **Add**. Then you'll see the newly entered hyperlink appear in the **Walled Garden Table**.

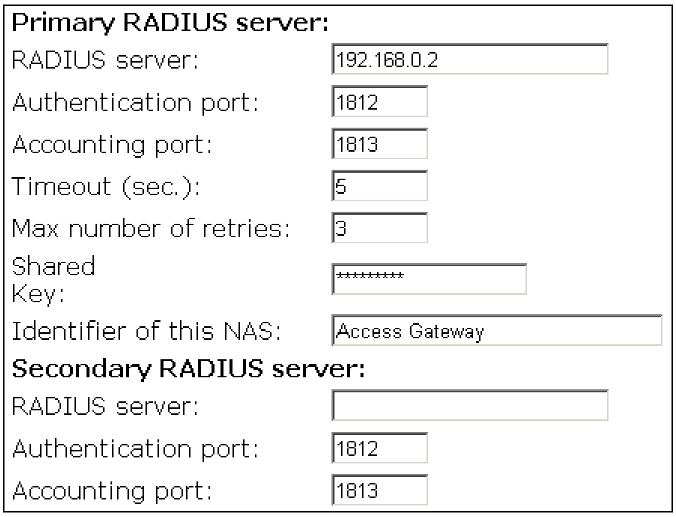
NOTE: You cannot specify a Web site that supports *Web redirection*, which redirects HTTP requests to another URL, as a walled garden site. If such a Web-redirection-enabled site is specified in the walled garden, an HTTP access request to this site is redirected to another site that is "out of" the walled garden. And the user is therefore needs to be authenticated to access this out-of-walled-garden site. Always specify a Web site that actually hosts Web content as a walled garden site.

TIP: You can also specify port numbers or port ranges for a walled gardened URL. Up to 4 port ranges are supported. For example, if you want an HTTPS-based walled garden entry, just specify port 443. The following are all valid inputs:

- www.xyz.com:8080/dir/subdir/
- www.xyz.com:443/dir/subdir/index.htm
- www.interepoch.com.tw:8080/subdir /index.htm,110,1024-1285

3.6.2. RADIUS

3.6.2.1. Basic



Primary RADIUS server:	
RADIUS server:	192.168.0.2
Authentication port:	1812
Accounting port:	1813
Timeout (sec.):	5
Max number of retries:	3
Shared Key:	*********
Identifier of this NAS:	Access Gateway
Secondary RADIUS server:	
RADIUS server:	
Authentication port:	1812
Accounting port:	1813

Fig. 87. RADIUS basic settings.

For the *advanced* wireless access gateway, the RADIUS client component of the gateway is shared by the IEEE 802.1x and Web redirection components. The RADIUS settings are for the RADIUS client to communicate with backend RADIUS servers.

NOTE: When configured for EAP authentication, the RADIUS server supports either EAP-TLS or EAP-MD5, but not both at the same time. As a result, not all combinations of EAP-MD5, EAP-TLS, PAP and CHAP authentication methods are available if both IEEE 802.1x and Web redirection are enabled. The following table shows the allowable IEEE 802.1x and Web redirection authentication modes on the *Wireless Advanced* edition of access gateway.

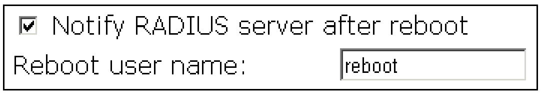
Table 2. Allowable authentication modes.

	IEEE 802.1x disabled	IEEE 802.1x EAP-MD5	IEEE 802.1x EAP-TLS
Web redirection disabled	■	■	■
Web redirection EAP-MD5	■	■	
Web redirection PAP	■	■	■
Web redirection CHAP	■	■	■

The gateway can be configured to communicate with two RADIUS servers. When the primary RADIUS server fails to respond, the gateway will try to communicate with the secondary RADIUS server. You can specify the length of timeout and the number of retries before communicating with the secondary RADIUS server after failing to communicate with the primary RADIUS server.

The gateway and its RADIUS server(s) share a secret key so that they can authenticate each other. In addition to its IP address, the gateway can identify itself by an NAS (Network Access Server) identifier. Each gateway must have a *unique* NAS identifier.

3.6.2.2. Robustness



☑ Notify RADIUS server after reboot

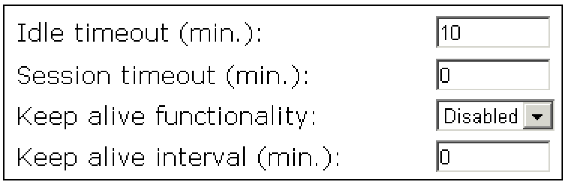
Reboot user name: reboot

Fig. 88. RADIUS robustness settings.

The gateway can be configured to notify the RADIUS server after it reboots. The RADIUS server can make use of the notification to clean up user authentication session records in the event that the gateway reboots unexpectedly due to abnormal operation.

Select the **Notify RADIUS server after reboot** check box to enable this capability, and then specify the name of the *pseudo user* (default to "reboot") for this operation in the **Reboot user name** text box.

3.6.3. Authentication Session Control



Idle timeout (min.): 10

Session timeout (min.): 0

Keep alive functionality: Disabled

Keep alive interval (min.): 0

Fig. 89. Authentication session control settings.

Authentication session control settings are for controlling the lifetimes of user authentication sessions. The **Idle timeout** setting specifies how long a user can be idle without generating any traffic before being terminated. The **Session timeout** setting specifies the maximum session lifetime.

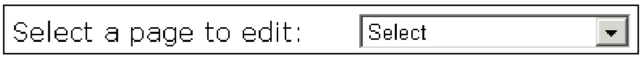
In addition, the gateway provides a mechanism for detecting whether a user has left unexpectedly by handshaking between JavaScript code in the *log-off* authentication page and the gateway. The *log-off* page notifies the gateway periodically to announce user existence. When this mechanism for user existence detection is enabled (**Keep alive functionality**), the gateway will terminate a user if no notification is received from the *log-off* page on the user's computer within the number of minutes specified by the **Keep alive interval** setting.

NOTE: A zero value in the **Idle timeout**, **Session timeout**, or **Keep alive interval** setting disables the corresponding functionality effectively.

NOTE: The **Log-Off** window cannot not be shown on a Windows CE-based Pocket PC due to different JavaScript behavior of Pocket Explorer. To support Windows CE-based clients, you have to *disable* the keep-alive mechanism; otherwise the clients will be terminated unexpectedly.

3.6.4. Authentication Page Customization

3.6.4.1. Selecting an Authentication Page to Edit



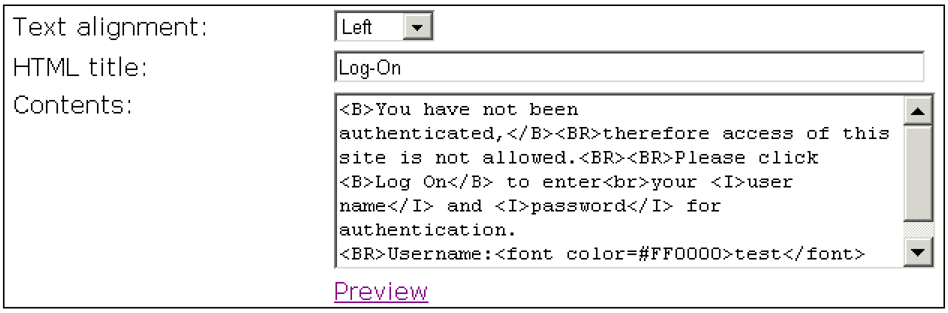
Select a page to edit: Select

Fig. 90. Selecting an authentication page to edit.

The 4 authentication pages—*log on*, *authentication success*, and *authentication failure*—stored on the gateway can be customized. Select a page to edit from the **Select a page to edit** drop-down list.

3.6.4.2. Log-On, Authentication Success, and Authentication Failure Pages

Log-on, *authentication success*, and *authentication failure* authentication pages can be customized in a similar way. You can specify the **Text alignment** style, page title (**HTML title**) and the **Contents**. The **Contents** setting accepts HTML tagging. Clicking the **Preview** link shows a test page for you to see the results.



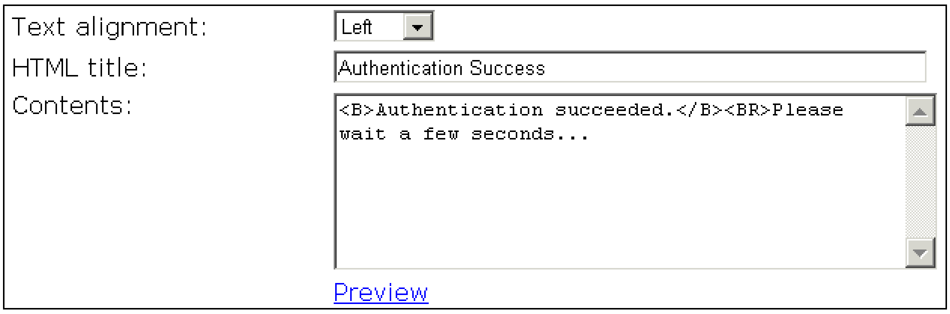
Text alignment: Left

HTML title: Log-On

Contents:

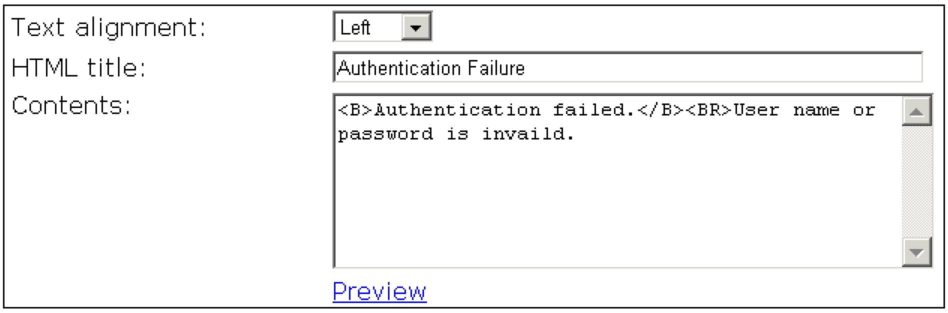
```
<B>You have not been
authenticated,</B><BR>therefore access of this
site is not allowed.<BR><BR>Please click
<B>Log On</B> to enter<br>your <I>user
name</I> and <I>password</I> for
authentication.
<BR>Username:<font color=#FF0000>test</font>
```

Fig. 91. Log-on page customization settings.



Text alignment:	Left
HTML title:	Authentication Success
Contents:	<B>Authentication succeeded.</B><BR>Please wait a few seconds...
	Preview

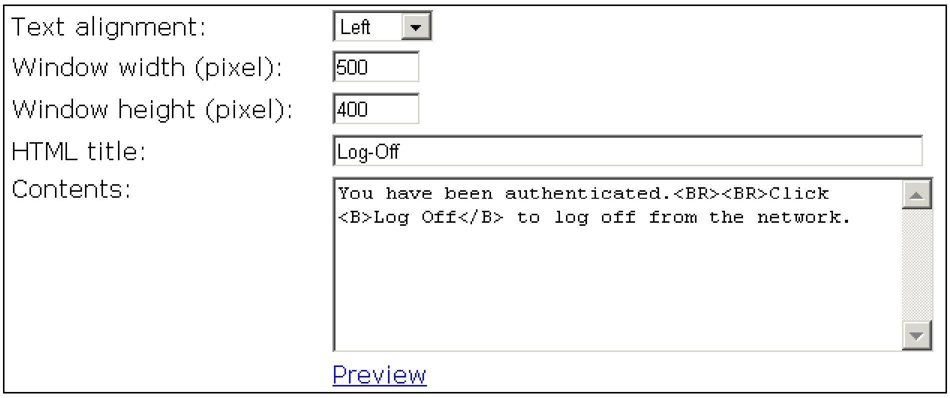
Fig. 92. Authentication success page customization settings.



Text alignment:	Left
HTML title:	Authentication Failure
Contents:	<B>Authentication failed.</B><BR>User name or password is invaild.
	Preview

Fig. 93. Authentication failure page customization settings.

In addition to the **Text alignment**, **HTML title**, and **Contents** setting, two more settings are provided for specifying the size of the **Log-Off** window (**Windows width** and **Window height**).



Text alignment:	Left
Window width (pixel):	500
Window height (pixel):	400
HTML title:	Log-Off
Contents:	You have been authenticated.<BR><BR>Click <B>Log Off</B> to log off from the network.
	Preview

Fig. 94. Log-off page customization settings.

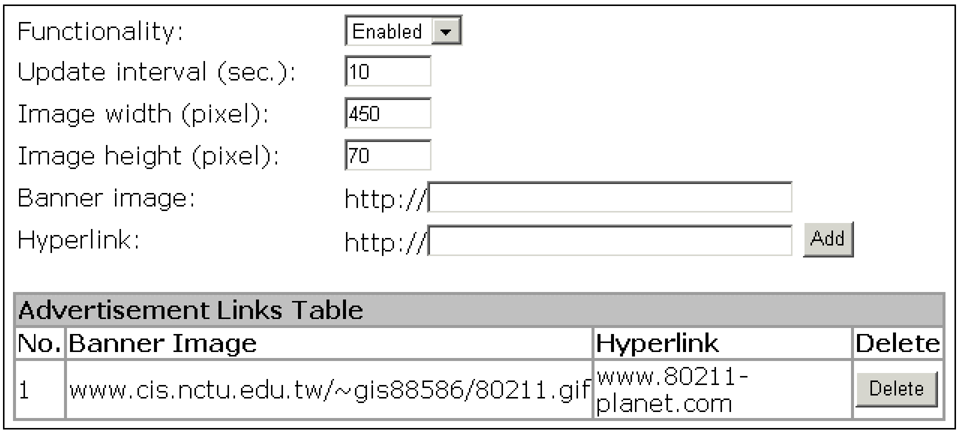
Furthermore, **Banner images** and **Hyperlinks** can be added to the **Log-Off** window for advertisement purposes. The banner images are shown in sequence at an interval specified by the **Update interval** setting. You can also specify the size of the banner image (**Image width** and **Image height**).

To specify an advertisement link:

1. Type the **Banner image** URL.

2. Type the **Hyperlink** URL.

3. Click the **Add** button, and then this advertisement link appears in the **Advertisement Links Table**.

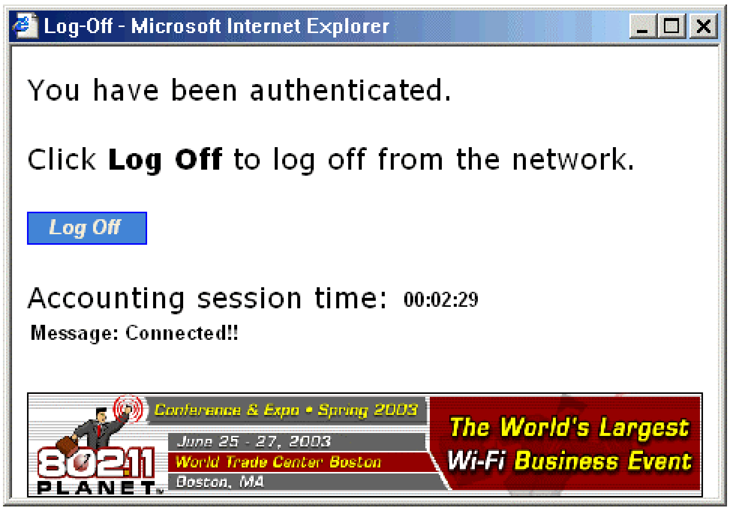


Functionality:	Enabled ▾
Update interval (sec.):	10
Image width (pixel):	450
Image height (pixel):	70
Banner image:	http://
Hyperlink:	http://

Advertisement Links Table

No.	Banner Image	Hyperlink	Delete
1	www.cis.nctu.edu.tw/~gis88586/80211.gif	www.80211-planet.com	Delete

Fig. 95. Advertisement links settings.



Log-Off - Microsoft Internet Explorer

You have been authenticated.

Click **Log Off** to log off from the network.

Accounting session time: **00:02:29**

Message: Connected!!

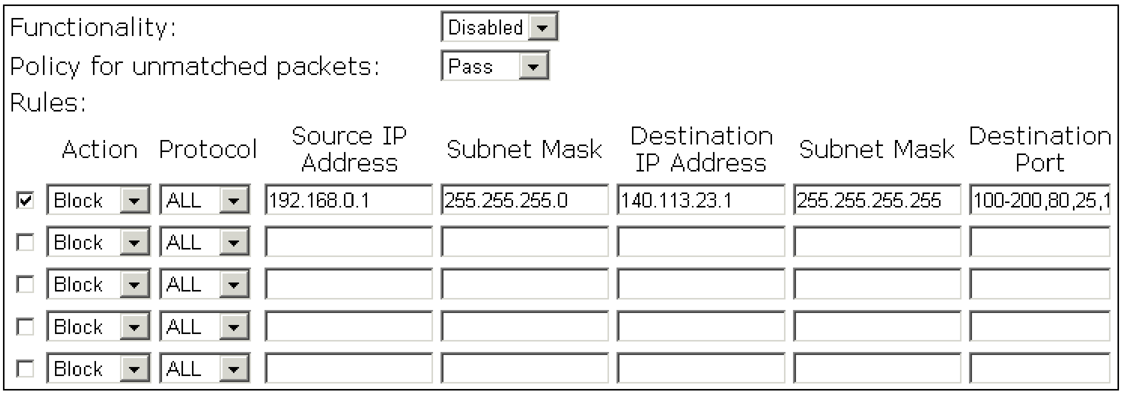
802.11 PLANET
Conference & Expo • Spring 2003
June 25 - 27, 2003
World Trade Center Boston
Boston, MA
The World's Largest
Wi-Fi Business Event

Fig. 96. Advertisement links in action.

3.7. Configuring Advanced Settings

3.7.1. Filters and Firewall

3.7.1.1. Packet Filters



Functionality: Disabled

Policy for unmatched packets: Pass

Rules:

	Action	Protocol	Source IP Address	Subnet Mask	Destination IP Address	Subnet Mask	Destination Port
☑	Block	ALL	192.168.0.1	255.255.255.0	140.113.23.1	255.255.255.255	100-200,80,25,1
☐	Block	ALL					
☐	Block	ALL					
☐	Block	ALL					
☐	Block	ALL					

Fig. 97. Packet filters settings.

You can specify rules for the firewall component of the gateway to check outgoing packets. Packets that meet the rules can be permitted or denied. The *protocol* field, *source IP address* field, *destination IP address* field, and *destination port* field of a packet's IP header are inspected to see if it meets a rule. A packet that *meets* a rule can be dropped (*Block*) or accepted (*Accept*) as specified in the **Action** setting of the rule. Packets that *do not meet* any rules can be dropped (*Discard*) or accepted (*Pass*) as specified in the **Policy** setting.

A rule is composed of 5 parts:

- What to do if a packet meets this rule (**Action**)
- Protocol type
  - All
  - ICMP
  - TCP
  - UDP
- Source IP address range (**Source IP Address** AND **Source Subnet Mask**)
- Destination IP address range (**Destination IP Address** AND **Destination Subnet Mask**)
- Port ranges

A source (destination) IP address range is determined by performing an AND operation on the source (destination) IP address field and the source (destination) subnet mask field. For example, if the source IP address field is 192.168.0.1 and the source subnet mask field is 255.255.255.0, the resultant source IP address range is 192.168.0.0 to 192.168.0.255.

Up to 5 port ranges can be specified in a rule, and these ranges must be separated by commas. For example, "21,80,85-89,140,200-230" in the destination port field signifies 5 port ranges.

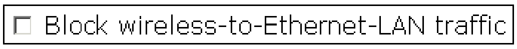
To set a rule for packet filtering:

1. Specify the **protocol** type, **source IP address**, **source IP mask**, **destination IP address**, **destination IP mask**, and **destination port** for the rule. Then specify in the **Action** setting how to deal with a packet that meets the rule.

2. Select the corresponding **Enabled** check box.

NOTE: Set the rules with great care since incorrect rules would make the gateway inaccessible. The last resort to restore the gateway to service may be resetting its configuration to factory-default values by pressing the **Default** switch on the housing of the gateway.

3.7.1.2. VLAN

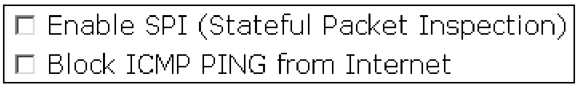


□ Block wireless-to-Ethernet-LAN traffic

Fig. 98. VALN settings.

VLAN (Virtual Local Area Network) settings are for traffic isolation. When the **Block wireless-to-Ethernet-LAN traffic** check box is selected, the gateway does not forward packets between the wireless network interface and the Ethernet LAN interface—traffic is allowed only between the Ethernet WAN interface and the wireless network interface.

3.7.1.3. Firewall



□ Enable SPI (Stateful Packet Inspection)
□ Block ICMP PING from Internet

Fig. 99. Packet filters and firewall settings.

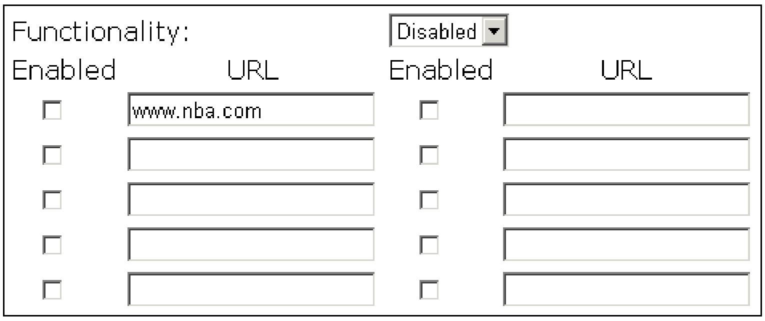
SPI analyzes incoming and outgoing packets based on a set of criteria for abnormal content. Therefore, SPI can detect hacker attacks, and can summarily reject an attack if the packet fits a suspicious profile. To enable SPI, select the **Enable Stateful Packet Inspection (SPI)** check box.

Some DoS (Denial of Service) attacks are based on sending invalid ICMP request packets to hosts. The gateway can be set to not accept any ICMP requests on the Ethernet WAN interface to defense against attacks of this kind. Enable this capability by selecting the **Block ICMP PING from Internet** check box.

NOTE: SPI can detect hacker attacks, including *IP-Spoofing*, *Zero IP Length*, *Land*, *Smurf*, *Fraggle*, *Teardrop*, *Ping of Death*, *Syn-Flood*, and *X-Tree*.

NOTE: Because some of the gateway's CPU resources are spent in checking packets for these security features, you may feel networking performance degradation if the security functions are enabled.

3.7.1.4. URL Filters



Functionality: Disabled ▾

Enabled	URL	Enabled	URL
□	www.nba.com	□	
□		□	
□		□	
□		□	
□		□	

Fig. 100. URL filters settings.

The gateway is capable of blocking HTTP traffic from the intranet to specified unwelcome Web sites.

To block HTTP traffic to an unwelcome Web site:

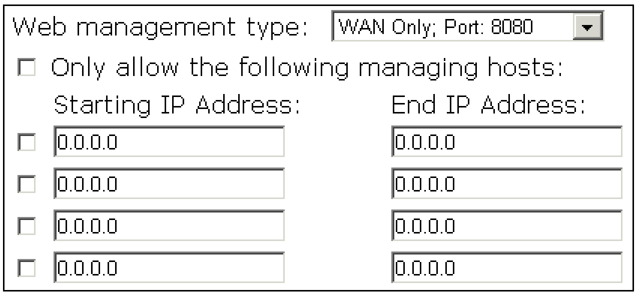
1. Specify the URL (ex. www.xxx.com) of the unwelcome Web site.

2. Select the corresponding **Enabled** check box.

NOTE: Do not type “http://” when specifying a URL. Just type the domain name.

3.7.2. Management

3.7.2.1. Basic



Web management type: WAN Only; Port: 8080 ▾

□ Only allow the following managing hosts:

	Starting IP Address:	End IP Address:
□	0.0.0.0	0.0.0.0
□	0.0.0.0	0.0.0.0
□	0.0.0.0	0.0.0.0
□	0.0.0.0	0.0.0.0

Fig. 101. Web-based management type setting.

The gateway can be managed locally from the LAN side, remotely from the WAN side, or from both sides. If the management type is **WAN Only** or **WAN and LAN**, be sure to specify the port **8080** when typing a URL for managing a gateway within a Web browser. For example, if the WAN interface of a gateway is configured to be 61.16.33.113, the URL for managing this gateway is “http://61.16.33.113:8080”.

In addition, if the management type is set to **WAN Only**, the gateway can be configured to be manageable only from specific hosts. In this way, security of remote management is enhanced.

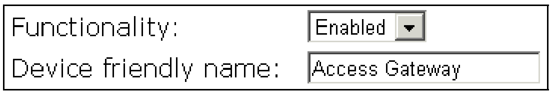
To make the gateway remotely manageable from specific hosts within an IP address range:

1. Select the **Only allow the following managing hosts** check box.

2. Type the **Starting IP address** and the **End IP Address** of the host IP address range.

3. Select the corresponding check box next to the IP address range.

3.7.2.2. UPnP



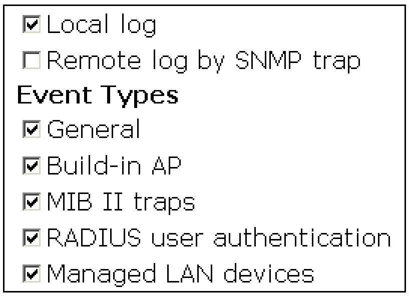
Functionality: Enabled ▾

Device friendly name: Access Gateway

Fig. 102. UPnP settings.

UPnP (Universal Plug and Play) enables a Windows XP user to automatically discover peripheral devices by HTTP. When the UPnP functionality is enabled, you can see the gateway in My Network Places of Windows XP. The gateway can be given a **friend name** that will be shown in My Network Places. *Double-clicking* the icon in My Network Places that stands for the gateway will launch the default Web browser for you to configure the gateway.

3.7.2.3. System Log



☑ Local log

□ Remote log by SNMP trap

Event Types

☑ General

☑ Build-in AP

☑ MIB II traps

☑ RADIUS user authentication

☑ Managed LAN devices

Fig. 103. System log settings.

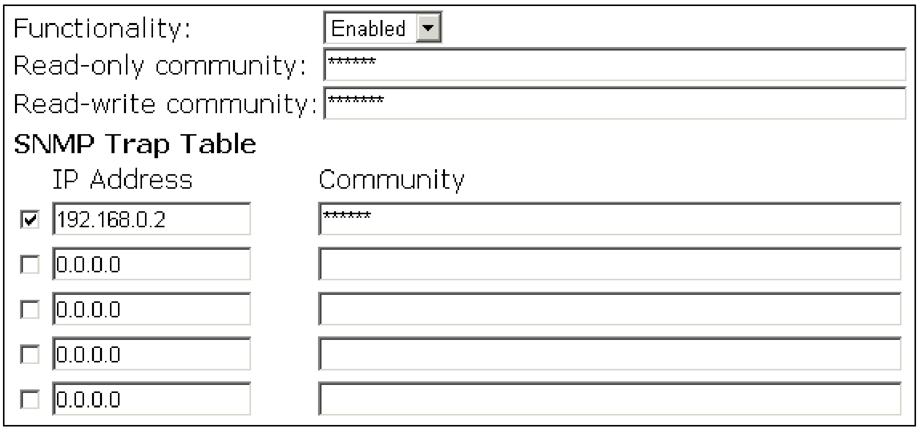
System events can be logged to the on-board RAM of the access gateway (**Local log**) or sent to a remote computer on which an SNMP trap monitor program runs (**Remote log by SNMP trap**). See the next subsection for more information about SNMP trap settings.

The system events are divided into the following categories:

- **General**: system and network connectivity status changes.
- **Built-in AP**: wireless client association and WEP authentication status changes.
- **MIB II traps**: *Cold Start*, *Warm Start*, *Link Up*, *Link Down* and *SNMP Authentication Failure*.
- **RADIUS user authentication**: RADIUS user authentication status changes.
- **Managed LAN devices**: managed LAN devices status changes (see Section 3.7.3 for more information).

NOTE: The *SNMP Authentication Failure* trap is issued when using an incorrect community string to manage the gateway via SNMP and the SNMP MIB II OID, **snmpEnableAuthenTraps**, is enabled (*disabled* by default).

3.7.2.4. SNMP



Functionality:	Enabled ▾
Read-only community:	******
Read-write community:	*******

SNMP Trap Table

	IP Address	Community
☑	192.168.0.2	******
□	0.0.0.0	
□	0.0.0.0	
□	0.0.0.0	
□	0.0.0.0	

Fig. 104. SNMP settings.

The gateway can be managed by SNMP (Simple Network Management Protocol), and the SNMP management functionality can be disabled. You can specify the name (used as a *password*) of the read-only and read-write community. In addition, up to 5 SNMP trap targets can be set in the **SNMP Trap table**.

To specify a trap target:

1. Type the IP address of the target host.

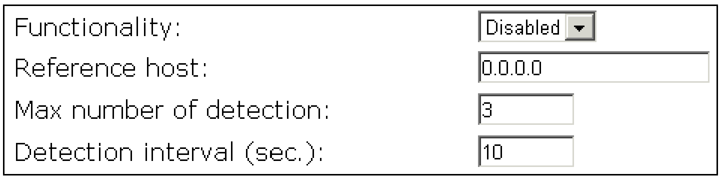
2. Type the **Community** for the host.

3. Select the corresponding check box next to the **IP address** text box.

3.7.3. Auto Recovery

In rare cases, the firmware of the access gateway gets stuck in an invalid state due to bugs in the firmware and the access gateway appears to be locked up from end user perspective. The access gateway is equipped with two software-based auto recovery mechanisms to solve lockup situations. The auto recovery mechanisms could be very useful for a WISP before a new version of firmware is released for bug fixes.

3.7.3.1. Link Integrity Detection

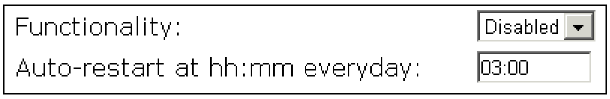


Functionality:	Disabled ▾
Reference host:	0.0.0.0
Max number of detection:	3
Detection interval (sec.):	10

Fig. 105. Link integrity detection settings.

The access gateway can be configured to ping a **Reference host** at intervals specified in **Detection interval**. If the access gateway cannot get any response after trying for the number of times specified in **Max number of detection**, it restarts. This mechanism is aimed at solving lockup caused by firmware bugs in the TCP/IP stack of the access gateway.

3.7.3.2. Periodical Restart

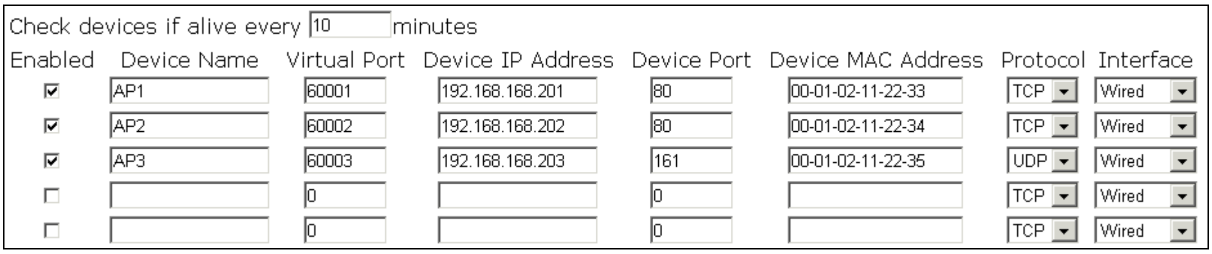


Functionality:	Disabled ▾
Auto-restart at hh:mm everyday:	03:00

Fig. 106. Periodical restart settings.

The access gateway can be configured to restart at a specific time every day. This mechanism is aimed at solving lockup caused by firmware bugs that surface only after the access gateway has operated for a long time. Specify the 24-hour time in **Auto-restart at hh:mm everyday** and enable **Functionality** to activate this auto recovery mechanism.

3.7.4. LAN Device Management



Check devices if alive every 10 minutes

Enabled	Device Name	Virtual Port	Device IP Address	Device Port	Device MAC Address	Protocol	Interface
☑	AP1	60001	192.168.168.201	80	00-01-02-11-22-33	TCP ▾	Wired ▾
☑	AP2	60002	192.168.168.202	80	00-01-02-11-22-34	TCP ▾	Wired ▾
☑	AP3	60003	192.168.168.203	161	00-01-02-11-22-35	UDP ▾	Wired ▾
□		0		0		TCP ▾	Wired ▾
□		0		0		TCP ▾	Wired ▾

Fig. 107. LAN device management settings.

LAN device management is for the access gateway to pass management requests from the Internet through its built-in NAT server to devices on the private network. As a result, network devices (such as access points) behind the NAT server can be managed from the Internet. In this way, the access gateway acts as a management proxy for the LAN devices. In addition, the gateway can periodically check whether the managed devices are working by PINGing them (**Check devices if alive every *n* minutes**). If it detects a device not working, it can send an SNMP trap (*remote system logging*) to a back-end server to report such a situation (see Section 3.7.2.3 for more information). The LAN device management functionality is especially useful for a WISP to remotely manage deployed APs that are usually invisible from the Internet due to the employment of NAT for IP address space conservation.

A management server from the Internet sees a managed LAN device as a combination of the access gateway's WAN IP address and a **Virtual Port** reserved for this device. When a TCP or UDP-based management request (specified by the **Protocol** field) is received by the access gateway from the Internet, the gateway translates the destination IP address and destination port of the request to the corresponding **Device IP Address** and **Device Port**. In other words, this request is passed through the built-in NAT server of the gateway and routed to the corresponding managed LAN device.

For example, Fig. 108 illustrates a LAN device management scenario based on the settings values in Fig. 107. AP1 can be managed from the management server by using a Web browser and a URL "http://61.16.31.110:60001". AP2 can be managed by using a Web browser and a URL "http://61.16.31.110:60002". AP3 can be managed from the management server by using an SNMP manager program via IP address 61.16.31.110 and port 60003. Destination IP addresses and destination ports of management packets for AP1, AP2, and AP3 are translated to 192.168.168.201:80, 192.168.168.202:80, and 192.168.168,201:161, respectively. (161 is a well known port for SNMP management.)

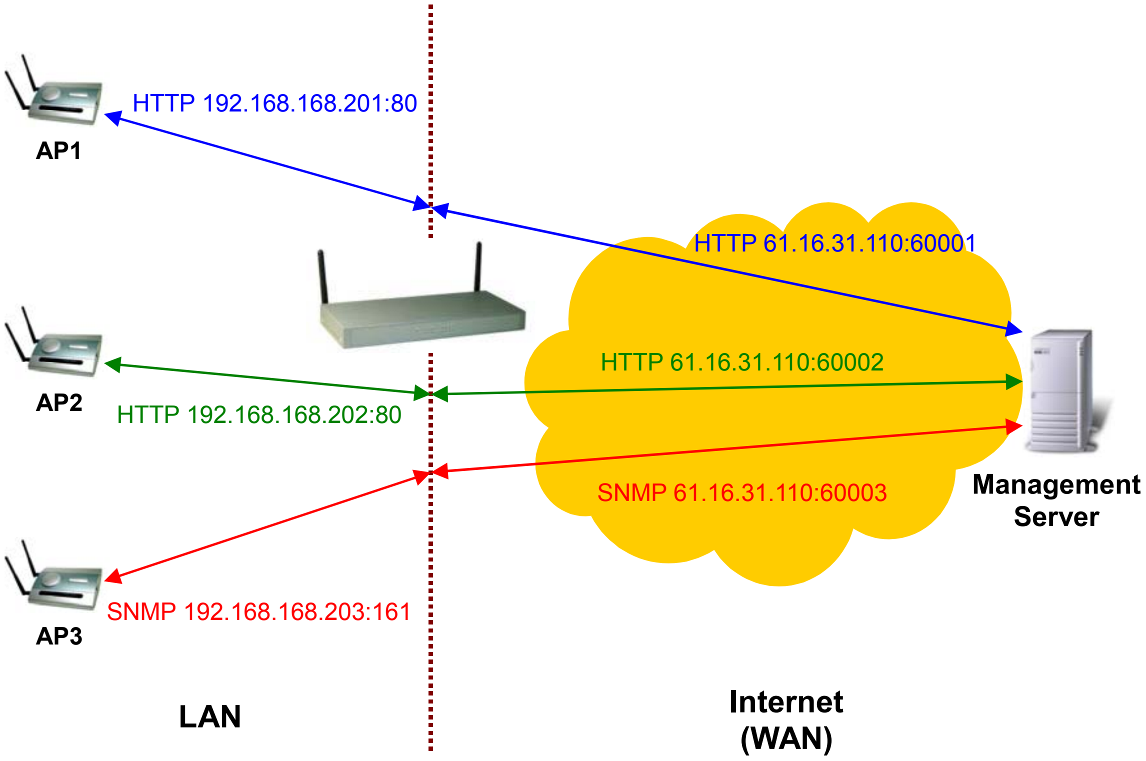


Fig. 108. Example for LAN device management.

To specify a LAN device to manage:

1. Give a name for this device in the **Device Name** text box.

2. Type the **Virtual Port**, **Device IP Address**, **Device Port**, and **Device MAC Address** for this device.

3. Choose the type of the management protocol (*TCP* or *UDP*) from the **Protocol** drop-down list.

4. Choose whether the gateway communicates with the device *wirelessly* by WDS (**Wireless**) or *by Ethernet* (**Wired**) from the **Interface** drop-down list.

5. Select the corresponding check box next to the **Device Name** text box.

NOTE: A valid input for the **Virtual Port** field must be between 60001 and 60100 inclusive.

NOTE: The IP address in a **Device IP Address** text box and the gateway's LAN IP address must be in the same IP subnet.

NOTE: The **Device Name**, **Device MAC Address**, and the **Interface** fields are informational. They do not affect the inner workings of LAN device management.

TIP: Alternatively, you can use a PPTP and Virtual Second LAN-based way for behind-NAT access point management. See Section 3.4.7 for more information.

Appendix A: Default Settings

TIP: Press the **Default** switch on the housing of a *powered-on* gateway to reset the configuration settings to factory-default values.

Setting Name	Default Value
Global	
User Name	root
Password	root
Operational Mode	Gateway with a Static-IP DSL/Cable Connection
IEEE 802.11b	
Regulatory Domain	FCC (U.S.)
Channel Number	11
SSID	wireless
SSID Broadcasts	Enabled
Transmission Rate	Auto
Transmit Power	High
MAC Address	See the label on the accompanying PCMCIA card or the label on the housing of the WLAN hotspot access gateway.
Security Mode	Open System
Selected WEP Key	Key #1
WEP Key #1	00-00-00-00-00
WEP Key #2	00-00-00-00-00
WEP Key #3	00-00-00-00-00
WEP Key #4	00-00-00-00-00
MAC-Address-Based Access Control	Disabled
Access Control Table Type	Inclusive
Wireless Client Isolation	Disabled
AP Load balancing	Disabled
WAN Interface	
Type	Static-IP DSL/Cable
Changeable MAC Address	Default MAC address of WAN interface
IP Address	192.168.100.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Host Name	gateway
Domain (DNS suffix)	Not set
PPP	
User Name	username
Password	Not set
Telephone Number	Not set
PPPoE	
User Name	username
Password	Not set
Service Name	servicename
LAN Interface	

Method of obtaining an IP Address	Set manually
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	
Functionality	Enabled
Default Gateway	192.168.0.1
Subnet Mask	255.255.255.0
Primary DNS Server	192.168.0.1
Secondary DNS Server	0.0.0.0
First Allocateable IP Address	192.168.0.2
Allocateable IP Address Count	20
NAT Server	
Functionality	Enabled
Virtual Server Mappings	Disabled
DMZ Host	Not set
Static NAT Mappings	Not set
DNS Proxy	
Static DNS Mappings	Not set
Filters/Firewall	
Packet Filters	Not set
URL Filters	Not set
VLAN	Disabled
WAN ICMP Request Blocking	Disabled
State Packet Inspection (SPI)	Disabled
Authentication	
Web Redirection	Disabled
RADIUS	Not set
RADIUS Robustness Reboot User Name	reboot
Session Control	Disabled
Management	
Web-Based Management Type	LAN only
SNMP	Enabled
SNMP Read-Only Community	public
SNMP Read-Write Community	private

Appendix B: Troubleshooting

Check the following first:

- Make sure that the power of the gateway is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the gateway.
- Make sure that the LED ALV of the gateway is blinking to indicate the gateway is working.
- Make sure the types of the Ethernet cables are correct. Recall that there are two types—*normal* and *crossover*.
- Make sure that the DSL, cable, V.90, or ISDN modem connected with the gateway is powered on.

B-1: TCP/IP Settings Problems

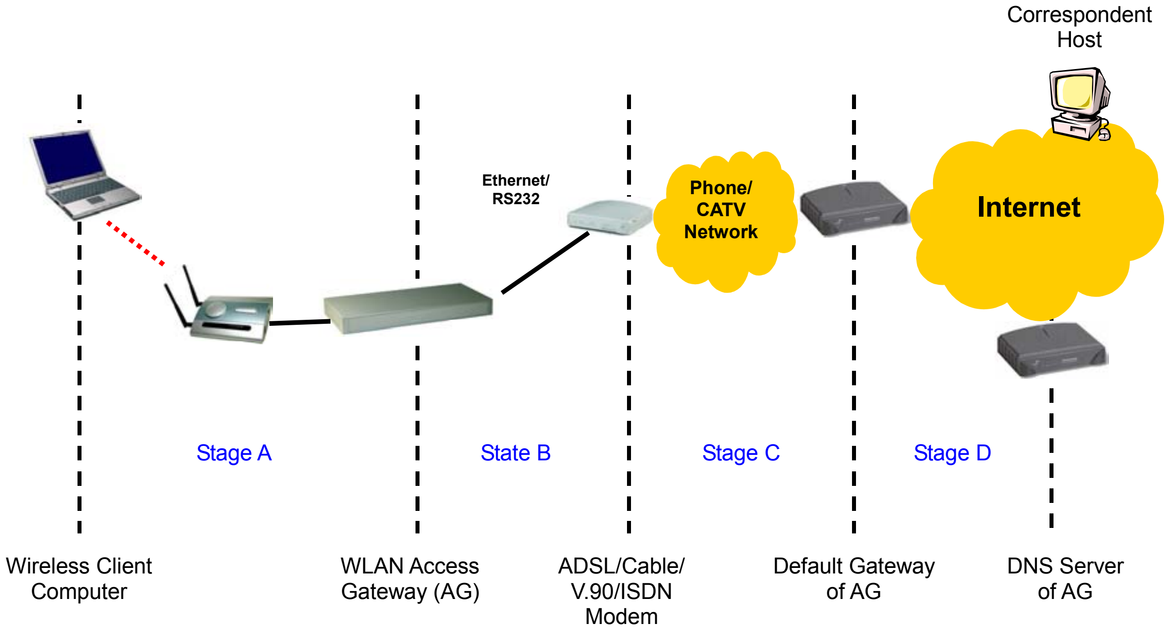


Fig. 109. Communication stages for a client to reach its correspondent host.

For a client computer to communicate with a correspondent host on the Internet by the host's domain name (e.g. http://www.wi-fi.com), it first sends a DNS request to a DNS server on the Internet. The DNS request travels first to the WLAN hotspot access gateway, then the WLAN hotspot access gateway relays this request to the default gateway of the WLAN hotspot access gateway through a modem. Finally, this request is forwarded by the default gateway to the DNS server on the Internet. The DNS reply issued by the DNS server is transmitted back to the client computer following a reverse path. When the client computer receives the DNS reply, it knows the IP address of the correspondent host and sends further packets to this IP address.

As illustrated in Fig. 109, the communication path could be broken at some of the stages. The OS-provided network diagnostic tool, **ping.exe**, can be employed to find out TCP/IP-related communication problems.

NOTE: If *two or more* NICs are installed and operating on a client computer, TCP/IP may not work properly due to incorrect entries in the routing table. Use the OS-provided command-line network tool, **route.exe**, to add or delete entries from the routing table. Or, use Windows-provided **Device Manager** to disable unnecessary NICs.

Solve the following problems in order:

- **The wireless client cannot pass Web redirection-based authentication.**
  - Are user name and password are correct?
    - Check the user credential information stored on the RADIUS server.
  - Is the RADIUS server correctly set up?
    - Check whether the password for the wireless client is stored using *reversible encryption* on the RADIUS server.
    - Check if the RADIUS server is set to use EAP-MD5, PAP, and CHAP authentication.
- **The WLAN hotspot access gateway does not respond to *ping* from the client computer.**
  - Are two or more NICs (wireless or wired) installed on the client computer?
    - Use the OS-provided command-line network tool, **route.exe**, to modify the contents of the routing table.
    - Use Windows-provided **Device Manager** to disable unnecessary NICs.
  - Is the underlying communication link established?
    - Make sure the wireless link is OK.
    - Make sure the Ethernet link between the AP and the WLAN hotspot access gateway is OK.
    - Make sure the settings of the client computer and of the WLAN hotspot access gateway match.
  - Are the IP address of the *client computer* and the IP address of the *WLAN hotspot access gateway* in the same IP subnet?
    - Use **WinIPCfg.exe** or **IPConfig.exe** to see the current IP address of the client computer. Make sure the IP address of the client computer and the IP address of the WLAN hotspot access gateway are in the same IP subnet.
    - **TIP:** If you forget the current IP address of the gateway, use Gateway/AP Browser to get the information (see Appendix B-2).
- **The default gateway of the WLAN hotspot access gateway does not respond to *ping* from the client computer.**
  - Solve the preceding problem first.

- Is the modem working?
  - You may find out the answer by directly connecting the modem to a computer. Referring to the manual of the modem if necessary.
- Are the IP address of the WLAN hotspot access gateway and the IP address of its default gateway in the same IP subnet?
  - Find out the answer on the start page of the Web-Based Network Manager.
- Is the NAT server functionality of the WLAN hotspot access gateway enabled?
  - Find out the answer on the start page of the Web-Based Network Manager.
- If you cannot find any incorrect settings of the WLAN hotspot access gateway, the default gateway of the WLAN hotspot access gateway may be really down or there are other communication problems on the network backbone.

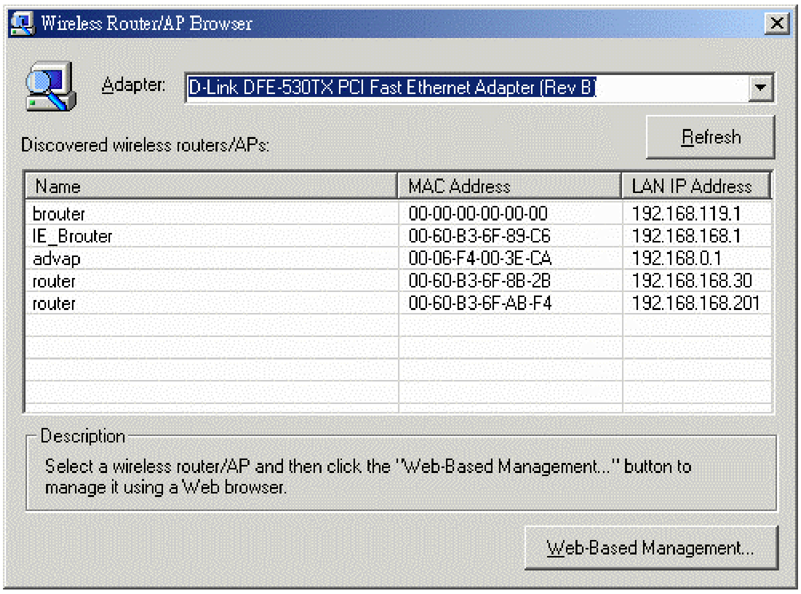
- **The DNS server(s) of the WLAN hotspot access gateway do not respond to *ping* from the client computer.**
  - Solve the preceding problems first.
  - If you cannot find any incorrect settings of the WLAN hotspot access gateway, the default gateway of the WLAN hotspot access gateway may be really down or there are other communication problems on the network backbone.

- **Cannot access the Internet.**
  - Solve the preceding problems first.
  - Make sure there are no incorrect packet filter settings that would block the traffic from the local computer to the Internet. In case you are not sure, the last resort may be resetting the configuration settings of the WLAN hotspot access gateway to default values by press the **Default** or **Soft-Reset** switch.

B-2: Other Problems

- **I forget the IP address of the LAN interface of the WLAN hotspot access gateway. What can I do to connect to it using a Web browser?**
  - Use the utility, Wireless Router/AP Browser (**WLBrwsr.exe**), in the "**Utilities**" folder on the companion CD-ROM disc. This utility can discover nearby WLAN APs, wireless routers, or WLAN hotspot access gateways and show their MAC addresses and IP addresses. In addition, it can launch the default Web browser on your computer.

NOTE: On Windows 2000/XP, Wireless Router/AP Browser can only be run by a user with administrator privilege.



Adapter: D-Link DFE-530TX PCI Fast Ethernet Adapter (Rev B)

Discovered wireless routers/APs:

Name	MAC Address	LAN IP Address
brouter	00-00-00-00-00-00	192.168.119.1
IE_Brouter	00-60-B3-6F-89-C6	192.168.168.1
advap	00-06-F4-00-3E-CA	192.168.0.1
router	00-60-B3-6F-8B-2B	192.168.168.30
router	00-60-B3-6F-AB-F4	192.168.168.201

Description

Select a wireless router/AP and then click the "Web-Based Management..." button to manage it using a Web browser.

Fig. 110. Gateway/AP Browser.

- **The WLAN hotspot access gateway stops working and does not respond to Web management requests.**

  - The firmware of the WLAN hotspot access gateway may be stuck in an incorrect state.

    - Press the **Reset** button on the housing of the WLAN hotspot access gateway or unplug the power connector from the power jack, and then re-plug the connector to restart the WLAN hotspot access gateway.

    - Contact our technical support representatives to report this problem, so that the bugs can be static in future firmware versions.

  - If the WLAN hotspot access gateway still does not work after restarting, there may be hardware component failures in the WLAN hotspot access gateway.

    - Contact our technical support representatives for repair.

Appendix C: Additional Information

C-1: Firmware Upgrade Using Xmodem Upgrade

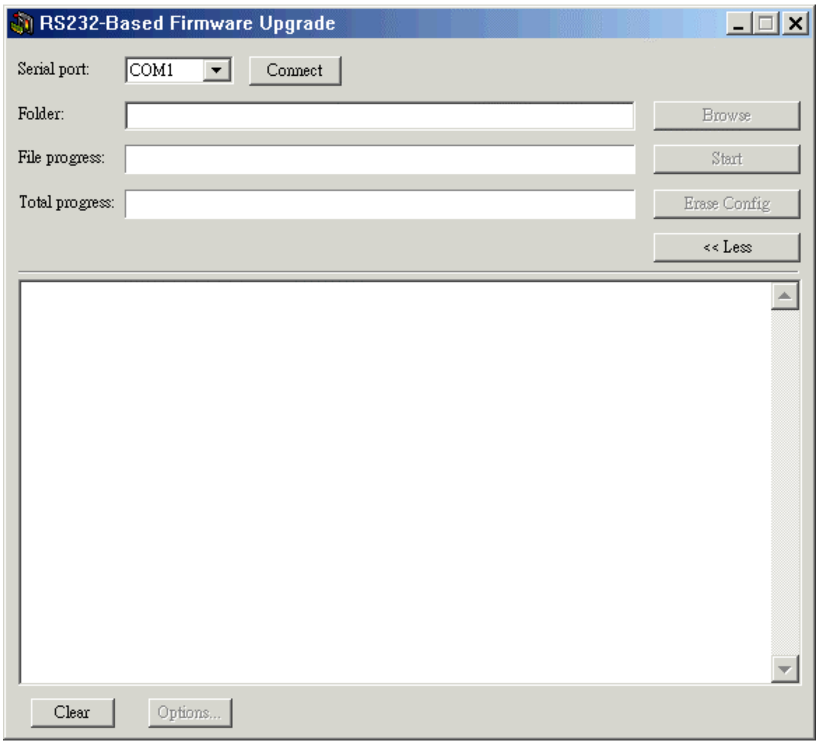


Fig. 111. Xmodem Upgrade.

To upgrade the firmware of WLAN hotspot access gateway using Xmodem Upgrade over RS232:

1. Power off the WLAN hotspot access gateway whose firmware will be upgraded.

2. Connect the managing PC and the WLAN hotspot access gateway with an *RS232 Null Modem* cable.

3. Select the serial port (COM1 or COM2) you use for connecting the device from the **Serial port** drop-down list and click **Connect**.

4. Chose the folder in which the firmware files reside by click **Browse**.

5. Power on the WLAN hotspot access gateway and you'll see bootup information.

6. Click **Start** to begin upgrade the firmware of the WLAN hotspot access gateway.

7. You will be prompted when the upgrade process completes.

Click **Erase Config** to reset the configuration settings of the WLAN hotspot access gateway to default values.

C-2: Distances and Data Rates

Important Notice: Maximum distances posted below are actual tested distance thresholds. However, there are many variables such as barrier composition and construction and local environmental interference that may impact your actual distances and cause you to experience distance thresholds far lower than those we post below.

IEEE 802.11b Maximum Distance Table				
Environmental Condition	**Speed and Distance Ranges**			
	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Open Environment: A "line-of-sight" environment with no interference or obstructions between Access Point and Users.	160 m (524 ft)	270 m (886 ft)	400 m (1312 ft)	457 m (1500 ft)
Semi-Open Environment: An environment with no major obstructions such as walls or privacy cubicles between Access Point and users.	50 m (164 ft)	70 m (230 ft)	90 m (295 ft)	120 m (394 ft)
Closed Environment: A typical office or home environment with floor to ceiling obstructions between Access Point and users.	25 m (82 ft)	35 m (115 ft)	45 m (148 ft)	55 m (180 ft)